MODULAR UNITS AND CUSPIDAL DIVISOR CLASS GROUPS OF $X_1(N)$

YIFAN YANG

ABSTRACT. In this article, we consider the group $\mathscr{F}_1^\infty(N)$ of modular units on $X_1(N)$ that have divisors supported on the cusps lying over ∞ of $X_0(N)$, called the ∞-cusps. For each positive integer N, we will give an explicit basis for the group $\mathscr{F}_1^\infty(N)$. This enables us to compute the group structure of the rational torsion subgroup $\mathscr{C}_1^\infty(N)$ of the Jacobian $J_1(N)$ of $X_1(N)$ generated by the differences of the ∞-cusps. In addition, based on our numerical computation, we make a conjecture on the structure of the p-primary part of $\mathscr{C}_1^\infty(p^n)$ for a regular prime p.

1. INTRODUCTION

Let Γ be a congruence subgroup of $SL(2, \mathbb{Z})$. A *modular unit* $f(\tau)$ on Γ is a modular function on Γ whose poles and zeros are all at cusps. If $\{\gamma_j\}$ is a set of right coset representatives of Γ in $SL(2, \mathbb{Z})$, then any symmetric sum of $f(\gamma_j \tau)$ is a modular function on $SL(2, \mathbb{Z})$ having poles only at ∞, whence a polynomial of the elliptic j-function. Hence, modular units are contained in the integral closure of the ring $\mathbb{C}[j]$. For arithmetic considerations, one may restrict his attention to the modular units that are in the integral closure of $\mathbb{Q}[j]$ or that of $\mathbb{Z}[j]$.

When $\Gamma = \Gamma_0(N)$, M. Newman [21, 22] determined sufficient conditions for a product $\prod_{d|N} \eta(d\tau)^{r_d}$ of Dedekind eta functions to be modular on $\Gamma_0(N)$. Because of the infinite product representation $\eta(\tau) = q^{1/24} \prod_{n=1}^\infty (1 - q^n)$, $q = e^{2\pi i \tau}$, such a modular function is a modular unit on $\Gamma_0(N)$. In [27], Takagi showed that for squarefree integers N, these functions generate the group of modular units on $\Gamma_0(N)$.

When $\Gamma = \Gamma(N)$ is the principal congruence subgroup of level N, the group of modular units on $\Gamma(N)$ has been studied extensively by Kubert and Lang in a series of papers [11, 12, 13, 14, 16]. Their main result states that the group of modular units on $\Gamma(N)$ is generated by (products of) the Siegel functions, except for 2-cotorsions in the case when N is an even composite integer. (See [10].) Note that here a 2-cotorsion of a subgroup H of a group G means an element g in G satisfying $g \notin H$, but $g^2 \in H$.

When $\Gamma = \Gamma_1(N)$, $N \geq 3$, Kubert and Lang [17, Chapter 3] consider a special subgroup $\mathscr{F}$ of modular units that have divisors supported at cusps lying over the cusp 0 of $X_0(N)$. A set of representatives for such cusps is

$$\{1/a : \ 1 \leq a \leq N/2, \ (a, N) = 1\}.$$

Because the homomorphism given by div : $f \mapsto \operatorname{div} f$ is injective modulo $\mathbb{C}^\times$, the maximal possible rank for this subgroup modulo $\mathbb{C}^\times$ is $\phi(N)/2 - 1$. In [17, Chapter 3], Kubert and Lang showed that this special subgroup does attain the maximal rank allowed. Moreover, they proved that this subgroup is generated by a certain class of the Siegel functions. Unlike the case $\Gamma(N)$, non-trivial cotorsions do not exist in this case.

The set of modular units is a very important object in number theory because of its wide range of applications. For example, the ray class field $K(\mathfrak{f})$ of conductor $\mathfrak{f}$ of an imaginary quadratic number field K can be obtained by adjoining the values, called the *Siegel-Ramachandra-Robert invariants*, of a suitable chosen modular unit on $\Gamma(N(\mathfrak{f}))$ at certain imaginary quadratic numbers, where $N(\mathfrak{f})$ denotes the smallest positive rational integer in $\mathfrak{f}$. (See Ramachandra [24].) The same Siegel-Ramachandra-Robert invariants also appeared earlier in the Kronecker limit formula for the L-functions associated with characters of the ray class group, originally due to C. Meyer [20]. Furthermore, in [25], Robert showed that suitable products of the Siegel-Ramachandra-Robert invariants are units, called *elliptic units*, in the ray class field $K(\mathfrak{f})$, and determined the index of the group of elliptic units in the full unit group of $K(\mathfrak{f})$ for the case $\mathfrak{f}$ is a power of prime ideal. The elliptic units featured prominently in Coates and Wiles' proof of (the weak form of) the Birch and Swinnerton-Dyer conjecture for the cases where elliptic curves have complex multiplication by the ring of integers in an imaginary quadratic field of class number one [2].

Another area in which modular units plays a fundamental role is the arithmetic of the Jacobian variety of a modular curve. Let Γ be a congruence subgroup of level N. Consider the cuspidal embedding $i_\infty : P \mapsto [(P) - (\infty)]$, sending a point P to the divisor class of $(P) - (\infty)$, of the modular curve $X(\Gamma)$ into its Jacobian $J(\Gamma)$. From the work of Manin and Drinfeld [18], we know that if P is a cusp, then $i_\infty(P)$ is a torsion point on $J(\Gamma)$. When the congruence subgroup Γ is $\Gamma_0(N)$ for some squarefree integer N, these points are actually rational points in $J_0(N) = J(\Gamma_0(N))$. For the case $N = p$ is a prime, Ogg [23] conjectured and Mazur [19] proved that the full rational torsion subgroup of $J_0(p)$ is generated by $i_\infty(0) = (0) - (\infty)$. Later on, in light of the Manin-Mumford conjecture (theorem of Raynaud), Coleman, Kaskel, and Ribet [3] proposed a stronger conjecture asserting that with the exception of hyperelliptic cases (excluding $p = 37$), if a modular curve $X_0(p)$ has genus greater than 1, then the only points on $X_0(p)$ that are mapped into torsion subgroups of $J_0(p)$ under i_∞ are the two cusps. This conjecture was later established by Baker [1].

For congruence subgroups of type $\Gamma_1(N)$, the images of cusps under the cuspidal embedding i_∞ are rational over $\mathbb{Q}(e^{2\pi i/N})$. Moreover, when the cusps P are lying over ∞ of $X_0(N)$, called the ∞-cusps, the images $i_\infty(P)$ are rational over $\mathbb{Q}$. In particular, these points $i_\infty(P)$ generate a rational torsion subgroup of $J_1(N)$. We shall denote this rational torsion subgroup by $\mathscr{C}_1^\infty(N)$. If we let $C_1^\infty(N)$ denote the set of ∞-cusps, $\mathscr{D}_1^\infty(N)$ the group of divisors of degree 0 generated by $C_1^\infty(N)$, and $\mathscr{F}_1^\infty(N)$ the group of modular units with divisors supported on $C_1^\infty(N)$, then the order of the $\mathscr{C}_1^\infty(N)$ is simply the divisor class number $h_1^\infty(N) := |\mathscr{D}_1^\infty(N)/\operatorname{div}\mathscr{F}_1^\infty(N)|$, which has been completely determined in literature. Firstly, the prime cases were settled by Klimek [9]. Then Kubert and Lang [15] considered the prime power cases p^n with $p \geq 5$. Finally, Yu [31] gave a class

number formula in full generality (given as Theorem A in the next section). Note that the divisor class number formulas in [17, Theorem 3.4] and [31] are stated as for the subgroup generated by the differences of the cusps lying over 0 of $X_0(N)$. However, it is plain that the Atkin-Lehner involution $\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$ gives rise to an isomorphism between the two divisor class groups.

It worths mentioning that the class number formula

$$h_1^\infty(p^n) = \prod_{\chi \neq \chi_0} \frac{1}{4} B_{2,\chi} \cdot \begin{cases} p^{p^{n-1}-2n+2}, & p \text{ odd}, \\ 2^{2^{n-1}-2n+3}, & p = 2, \end{cases}$$

for the prime power cases suggests that there exists an Iwasawa theory of $\mathbb{Z}_p$-extensions for the p-parts of $\mathscr{C}_1^\infty(p^n)$. The $\mathbb{Z}_p$-extension cannot be coming from the covering $X_1(p^{n+1}) \to X_1(p^n)$ as the covering is not even Galois. However, it is still possible to define a $\mathbb{Z}_p$-action on the sets $C_1^\infty(p^n)$ of ∞-cusps. This in turn induces a $\mathbb{Z}_p$-action on the divisor class groups $\mathscr{C}_1^\infty(p^n)$. We plan to address the Iwasawa properties of the p-parts of $\mathscr{C}_1^\infty(p^n)$ in the future, cf. the conjecture below.

With the order of $\mathscr{C}_1^\infty(N)$ determined, it is natural to ask the following questions:

(1) Is $\mathscr{C}_1^\infty(N)$ the full rational torsion subgroup of $J_1(N)$ when the ∞-cusps are the only cusps whose images in $J_1(N)$ are rational over $\mathbb{Q}$?

(2) What is the group structure of $\mathscr{C}_1^\infty(N)$? In particular, what is the structure of the p-primary part in the case $N = p^n$ is a prime power?

For the case $N = p$ is a prime, Conrad, Edixhoven, and Stein [4, Section 6.1] devised an algorithm to obtain an upperbound for the order of the rational torsion subgroup of $J_1(p)$. Comparing the upperbound with Kubert and Lang's divisor class number formula, they found that for $p < 157$ not equal to 29, 97, 101, 109, 113, the upperbound agrees with the divisor class number. In other words, in those cases $\mathscr{C}_1^\infty(p)$ is the whole rational torsion subgroup. Based on this numerical evidence, Conrad, Edixhoven, and Stein [4, Page 392] conjectured that for a prime $p \geq 5$, any rational torsion point on $J_1(p)$ is contained in the subgroup generated by the images of ∞-cusps under i_∞.

For the second question about the structure of $\mathscr{C}_1^\infty(N)$, the problem eventually boils down to the problem of finding a basis for the group $\mathscr{F}_1^\infty(N)$ of modular units. In [5] Csirik determined the structure of $\mathscr{C}_1^\infty(p)$ for the first few primes p. Presumably, he should have a method or an algorithm for finding a basis for $\mathscr{F}_1^\infty(p)$. Beyond [5], it appears that nothing is known in literature.

In this article, for each integer N greater than 4, we will construct an explicit basis for the group $\mathscr{F}_1^\infty(N)$ in terms of the Siegel functions. We will use two different methods in obtaining our results, depending on whether N is a prime power. When $N = p^n$ is a prime power, we use Yu's class number formula (Theorem A below) and linear algebra arguments to show that our basis does generate the whole group of modular units. When N is not a prime power, we use Yu's characterization of $\mathscr{F}_1^\infty(N)$ (Theorem B below) to argue directly that every function in $\mathscr{F}_1^\infty(N)$ is a product of functions from our basis. In either case, the so-called distribution relations (Lemma 5) play an essential role.

We then carry out some numerical computation on the structure of $\mathscr{C}_1^\infty(N)$ for N in the range of a few hundreds. This amounts to computing the Smith normal form of the matrix representing the divisors of the modular units in the basis. We have also computed the structure of the p-primary part of $\mathscr{C}_1^\infty(p^n)$ for $p^n < 800$ with $p = 2, 3, 5, 7$. Based on our limited numerical data (see Section 5), we make

the following conjecture about the structure of the p-primary part of $\mathscr{C}_1^\infty(p^n)$ for a regular prime p.

Conjecture. *Let p be a prime and n be a positive integer. Consider the endomorphism $[p] : \mathscr{C}_1^\infty(p^n) \to \mathscr{C}_1^\infty(p^n)$ defined by multiplication by p. Define the p-rank of $\mathscr{C}_1^\infty(p^n)$ to be the integer k such that the kernel of $[p]$ has p^k elements. If p is a regular prime, then we conjecture that the p-rank of $\mathscr{C}_1^\infty(p^n)$ is*

$$\frac{1}{2}(p-1)p^{n-2} - 1$$

for prime power $p^n \geq 8$ with $n \geq 2$.

More precisely, for a prime power $p^n \geq 8$ with a regular prime p, we conjecture that the the number of copies of $\mathbb{Z}/p^{2k}\mathbb{Z}$ in the primary decomposition of $\mathscr{C}_1^\infty(p^n)$ is

$$\begin{cases} \frac{1}{2}(p-1)^2 p^{n-k-2} - 1, & \text{if } p = 2 \text{ and } k \leq n - 3, \\ \frac{1}{2}(p-1)^2 p^{n-k-2} - 1, & \text{if } p \geq 3 \text{ and } k \leq n - 2, \\ \frac{1}{2}(p-5), & \text{if } p \geq 5 \text{ and } k = n - 1, \\ 0, & \text{else.} \end{cases}$$

and the number of copies of $\mathbb{Z}/p^{2k-1}\mathbb{Z}$ is

$$\begin{cases} 1, & \text{if } p = 2 \text{ and } k \leq n - 3, \\ 1, & \text{if } p = 3 \text{ and } k \leq n - 2, \\ 1, & \text{if } p \geq 5 \text{ and } k \leq n - 1, \\ 0, & \text{else.} \end{cases}$$

For powers of irregular primes, since the first case $N = 37^2$ has already exceeded our computational capacity, we do not have any numerical data to make any informed conjecture. However, we expect that the structure of the p-primary part of $\mathscr{C}_1^\infty(p^n)$ for such cases should still possess similar patterns. It would be very interesting to see if the same phenomenon also appears in the case of $\mathbb{Z}_p$-extension of number fields and function fields over finite fields.

The rest of the article is organized as follows. In Section 2, we explain our methods in details. In particular, we will review the basic properties of the Siegel functions, and then describe how we put Yu's theorems to use. In Sections 3 and 4, we consider the prime power cases and non-prime power cases, respectively. The prime cases, the odd prime power cases, and the power of 2 cases are dealt with separately in Theorems 1, 2, and 3. In Theorem 4 of Section 4, we consider the squarefree composite cases. Finally, in Theorem 5 we present bases for the remaining cases. Note that even though Theorem 4 is just a special case of Theorem 5, because the construction of bases in those cases is signicantly simpler and more transparent, those cases are handled separately to give the reader a clearer picture. Because of the complexity of our bases, many examples will be given. Finally, in Section 5, we give the results of our computation on the structures of of $\mathscr{C}_1^\infty(N)$ for $N \leq 100$. The structures of the p-primary parts of $\mathscr{C}_1^\infty(p^n)$ are also given for $p^n \leq 800$ with $p = 2, 3, 5, 7$, along with a few cases of $\mathscr{C}_1^\infty(mp^n)$.

2. Methodology

2.1. Notations and conventions.

In this section, we will collect all the notations and conventions that will be used throughout the paper.

Foremost, the letter N will be reserved exclusively for the level of the congruence subgroup $\Gamma_1(N)$ that is under our consideration. For $N \geq 5$, we let

$C_1^\infty(N) =$ the set of cusps of $X_1(N)$ lying over ∞ of $X_0(N)$,

$\mathscr{D}_1^\infty(N) =$ the group of divisors of degree 0 on $X_1(N)$ having support on $C_1^\infty(N)$,

$\mathscr{F}_1^\infty(N) =$ the group of modular units on $X_1(N)$

  having divisors supported on $C_1^\infty(N)$,

$\mathscr{C}_1^\infty(N) =$ the divisor class group $\mathscr{D}_1^\infty(N)/\operatorname{div}\mathscr{F}_1^\infty(N)$,

$h_1^\infty(N) = |\mathscr{D}_1^\infty(N)/\operatorname{div}\mathscr{F}_1^\infty(N)|$, the divisor class number.

Given a Dirichlet character χ modulo N, we let $B_{k,\chi}$ denote the generalized Bernoulli numbers defined by the power series

$$\sum_{a=1}^{N} \chi(a) \frac{te^{at}}{e^{Nt}-1} = \sum_{k=0}^{\infty} \frac{B_{k,\chi}}{k!} t^k.$$

In particular, if we let $\{x\}$ be the fractional part of a real number x, then we have

$$B_{2,\chi} = N \sum_{a=1}^{N} \chi(a) B_2(a/N),$$

where

$$B_2(x) = \{x\}^2 - \{x\} + \frac{1}{6}$$

is the second Bernoulli function. Note that some authors define generalized Bernoulli numbers slightly differently. If an imprimitive Dirichlet character χ has conductor f and let χ_f be the character modulo f that induces χ, then in [31] the Bernoulli number associated with χ is defined as

$$(1) \qquad \frac{f}{2} \sum_{a=1}^{f} \chi_f(a) B_2(a/f),$$

which is $B_{2,\chi_f}/2$ in our notation. The numbers $B_{2,\chi}$ and B_{2,χ_f} are connected by the formula

$$B_{2,\chi} = B_{2,\chi_f} \prod_{p|N,\ p\nmid f} (1 - \chi_f(p)p),$$

proved in (9) below.

We now introduce the Siegel functions. For $a = (a_1, a_2) \in \mathbb{Q}^2$, $a \notin \mathbb{Z}^2$, the Siegel functions $g_a(\tau)$ are usually defined in terms of the Klein forms and the Dedekind eta functions. For our purpose, we only need to know that they have the following infinite product representation. Setting $z = a_1\tau + a_2$, $q_\tau = e^{2\pi i\tau}$, and $q_z = e^{2\pi iz}$, we have

$$g_a(\tau) = -e^{2\pi i a_2(a_1-1)/2} q_\tau^{B(a_1)/2}(1 - q_z) \prod_{n=1}^{\infty} (1 - q_\tau^n q_z)(1 - q_\tau^n/q_z),$$

where $B(x) = x^2 - x + 1/6$ is the second Bernoulli polynomial. These functions, without the exponential factor $-e^{2\pi i a_2(a_1-1)/2}$, are sometimes referred to as generalized Dedekind eta functions by some authors, notably [26, Chapter VIII].

For a given integer N, we also define a class of functions

$$E_a^{(N)}(\tau) = -g_{(a/N,0)}(N\tau) = q^{NB(a/N)/2} \prod_{n=1}^{\infty} \left(1 - q^{(n-1)N+a}\right)\left(1 - q^{nN-a}\right),$$

for integers a not congruent to 0 modulo N, where $q = e^{2\pi i\tau}$. The basic properties of $E_a^{(N)}(\tau)$ will be introduced in the next section. They will be the building blocks of our bases. In a loose sense, we say these functions are functions of *level N*. (It does not mean that $E_a^{(N)}$ by itself is modular on some congruence subgroup of level N, but that we use them to construct modular functions on $\Gamma_1(N)$. However, the $12N$th power of $E_a^{(N)}$ is indeed modular on $\Gamma_1(N)$.) Notice that if $d|(a, N)$, then we have the trivial relation

$$E_a^{(N)}(\tau) = E_{a/d}^{(N/d)}(d\tau).$$

From time to time, we will write $E_{a/d}^{(N/d)}(d\tau)$ in place of $E_a^{(N)}(\tau)$ to stress the point that such a function is really coming from a congruence subgroup of lower level. Also, the notation $E_a(\tau)$ without the superscript has the same meaning as $E_a^{(N)}(\tau)$.

Note that it is easy to check that $E_{g+N} = E_{-g} = -E_g$. Therefore, for a given N, there are only $\lceil (N-1)/2 \rceil$ essentially distinct E_g, indexed over the set $(\mathbb{Z}/N\mathbb{Z})/\pm 1 - \{0\}$. Thus, a product $\prod_g E_g^{e_g}$ is understood to be taken over $g \in (\mathbb{Z}/N\mathbb{Z})/\pm 1 - \{0\}$.

Finally, for a divisor K of N, the group $\mathbb{Z}/K\mathbb{Z}$ acts on $(\mathbb{Z}/N\mathbb{Z})/\pm 1$ naturally by $a \mapsto a + kN/K$ for $a \in (\mathbb{Z}/N\mathbb{Z})/\pm 1$ and $k \in \mathbb{Z}/K\mathbb{Z}$. We let

$$\mathcal{O}_{a,K} := \{b \in \mathbb{Z}/N\mathbb{Z} : \ a \equiv b \mod N/K\}/\pm 1$$

be the orbit of a under this group action.

2.2. **Properties of Siegel functions.** In this section, we collect properties of the functions $E_g^{(N)} = E_g$ relevant to our consideration. The proof of these properties can be found in [30]. Throughout the section, N is a fixed integer greater than 4.

The first property given is the transformation law for E_g.

Proposition 1 ([30, Corollary 2]). *The functions E_g satisfy*

(2) $$E_{g+N} = E_{-g} = -E_g.$$

Moreover, let $\gamma = \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N)$. We have, for $c = 0$,

$$E_g(\tau + b) = e^{\pi ibNB(g/N)} E_g(\tau),$$

and, for $c > 0$,

(3) $$E_g(\gamma\tau) = \epsilon(a, bN, c, d)e^{\pi i(g^2 ab/N - gb)}E_{ag}(\tau),$$

where

$$\epsilon(a, b, c, d) = \begin{cases} e^{\pi i(bd(1-c^2)+c(a+d-3))/6}, & \text{if } c \text{ is odd,} \\ -ie^{\pi i(ac(1-d^2)+d(b-c+3))/6}, & \text{if } d \text{ is odd.} \end{cases}$$

Remark. The proof of this property given in [30] used the transformation formula for the Jacobi theta function $\vartheta_1(z|\tau)$. An alternative approach will be to use the fact that the Siegel function is equal to the product of the Klein form and $\eta(\tau)^2$. Then from the fact that the Klein form is a form of weight -1 on $SL(2, \mathbb{Z})$ and the transformation formula for $\eta(\tau)$ ([29, pp. 125–127]), one can deduce the above formula for E_g. The advantage of the argument given in [30] is that it can be generalized to the case of Jacobi forms (see [6] for the definition and properties of Jacobi forms) and the Riemann theta functions of higher genus.

From the transformation law, we immediately obtain sufficient conditions for a product $\prod_g E_g^{e_g}$ to be modular on $\Gamma_1(N)$.

Proposition 2 ([30, Corollary 3]). *Consider a function $f(\tau) = \prod_g E_g(\tau)^{e_g}$, where g and e_g are integers with g not divisible by N. Suppose that one has*

(4) $$\sum_g e_g \equiv 0 \mod 12, \qquad \sum_g ge_g \equiv 0 \mod 2$$

and

(5) $$\sum_g g^2 e_g \equiv 0 \mod 2N.$$

Then f is a modular function on $\Gamma_1(N)$.

Furthermore, for the cases where N is a positive odd integer, conditions (4) and (5) can be reduced to

$$\sum_g e_g \equiv 0 \mod 12$$

and

$$\sum_g g^2 e_g \equiv 0 \mod N,$$

respectively.

The following proposition gives the order of E_g at cusps of $X_1(N)$.

Proposition 3 ([30, Lemma 2]). *The order of the function E_g at a cusp a/c of $X_1(N)$ with $(a, c) = 1$ is $(c, N)B_2(ag/(c, N))/2$, where $B_2(x) = \{x\}^2 - \{x\} + 1/6$ and $\{x\}$ denotes the fractional part of a real number x.*

From the above proposition, we can easily see that when $N = p$ is a prime, any quotient E_{g_1}/E_{g_2} will have a divisor (with rational coefficients) supported on $C_1^\infty(p)$. For general N, after a moment of thought, we find the following condition for a product $\prod_g E_g^{e_g}$ to have a divisor supported on $C_1^\infty(N)$.

Lemma 4 ([31, Lemma 4.1]). *Let N be a positive composite integer. If $f(\tau) = \prod_g E_g^{e_g}$ satisfies the orbit condition*

$$\sum_{g \in \mathcal{O}_{a,p}} e_g = 0$$

for all $a \in \mathbb{Z}/N\mathbb{Z}$ and all prime divisors p of N, then the poles and zeros of $f(\tau)$ occur only at cusps lying over ∞ of $X_0(N)$.

In fact, Yu [31], cited as Theorem B below, showed that when N has at least two distinct prime factors, the orbit condition is the necessary and sufficient condition for $\prod_g E_g^{e_g}$ to be a modular unit contained in $\mathscr{F}_1^\infty(N)$. (For prime power cases $N = p^n$, a function satisfying the orbit condition alone will still have a divisor supported on $C_1^\infty(p^n)$, but the orders at cusps may not be integers.)

Finally, we need the following distribution relations among E_g and among generalized Bernoulli numbers.

Lemma 5. *Assume that $N = nM$ for some positive integer n. Then we have for all integers a with $0 < a < M$,*

$$(6) \qquad N \sum_{k=0}^{n-1} B_2 \left(\frac{kM + a}{N} \right) = M B_2 \left(\frac{a}{M} \right),$$

and consequently

$$\prod_{k=0}^{n-1} E_{kM+a}^{(N)}(\tau) = E_a^{(M)}(\tau).$$

Proof. The proof of the first statement is a straightforward computation. Then the second statement follows immediately from (6) and the definition of $E_a^{(M)}$. $\square$

Remark. Relation (6) shows that the set of all numbers $N B_2(a/N)$ forms a distribution, called the *Bernoulli distribution*. See [28, Chapter 12] and [17, Chapter 1].

2.3. **Method for prime power cases.** Let $N = p^n$ be a prime power. In this section we will explain how to use the following result of Yu to obtain a basis for $\mathscr{F}_1^\infty(N)$. Note that in the formula, if an imprimitive Dirichlet character χ modulo N has conductor f, we let χ_f denote the character modulo f that induces χ.

Theorem A ([31, Theorem 5]). *Let $N \geq 5$ be a positive integer and $\omega(N)$ be the number of distinct prime divisors of N. For a prime divisor p of N, let $p^{n(p)}$ be the highest power of p dividing N. We have the class number formula*

$$(7) \qquad h_1^\infty(N) = \prod_{p|N} p^{L(p)} \prod_{\chi \neq \chi_0 \ even} \left(\frac{1}{4} B_{2,\chi_f} \prod_{p|N} (1 - p^2 \chi_f(p)) \right)$$

for $h_1^\infty(N) = |\mathscr{D}_1^\infty(N)/\operatorname{div} \mathscr{F}_1^\infty(N)|$, where

$$L(p) = \begin{cases} \phi(N/p^{n(p)})(p^{n(p)-1} - 1) - 2n(p) + 2, & \text{if } \omega(N) \geq 2, \\ p^{n-1} - 2n + 2, & \text{if } N = p^n \text{ and } p \text{ is odd,} \\ 2^{n-1} - 2n + 3, & \text{if } N = 2^n \geq 8, \end{cases}$$

and the product $\prod_\chi$ runs over all even non-principal Dirichlet characters modulo N.

Remark. Note that the definition of the generalized Bernoulli numbers used in [31] is different from ours. See Section 2.1 for details.

In [31], the number $L(p)$ in the class number formula is given as

$$L(p) = \begin{cases} \phi(N/p^{n(p)})(p^{n(p)-1} - 1) - 2n(p) - 2, & \text{if } N \text{ is composite,} \\ p^{n-1} - 2n - 2, & \text{if } N = p^n > 4. \end{cases}$$

As pointed out in [8], the minus sign in front of 2 is an obvious misprint. Also, the use of the term "composite" in [31] is somehow unconventional as it refers to an integer N with $\omega(N) > 1$ throughout [31].

The discrepancy in the case $N = 2^n$ is due to a slight oversight in the proof of Lemma 3.4 of [31]. Upon a close examination, one can see that when $N = 2^n$, Lemma 3.4 of [31] is valid only in the range $3 \le \ell \le n$, not $2 \le \ell \le n$. Note that when $N = 2^3$, Yu's formula actually gives

$$2^{2^2-6+2} \cdot \frac{1}{4} \cdot 8 \cdot (B_2(1/8) - B_2(3/8) - B_2(5/8) + B_2(7/8)) = \frac{1}{2}$$

as the class number, which clearly can not be the correct number.

Remark. In [8], Hazama gave another class number formula for $h_1^\infty(N)$ for $N \not\equiv 0$ mod 4 in terms of the so-called Demjanenko matrix. The new formula is more or less a result of manipulation of the generalized Bernoulli numbers. It does not give a new proof of Yu's formula. Nonetheless, Hazama's formula will be useful in verifying the correctness of our numerical computation. However, the reader should be mindful of several errors when applying Hazama's formula.

In the statement of Theorem 3.1 of [8], f_i should be defined as the multiplicative order of p_i in $(\mathbb{Z}/m_i\mathbb{Z})^\times / \pm 1$, not $(\mathbb{Z}/m_i\mathbb{Z})^\times$, and e_i should be $\phi(m_i)/(2f_i)$. Then $A_{p_i}(m)$ is simply $(1 + p_i^{f_i})^{e_i}/(1 + p_i)$. The quantities f, e, $A(m)$ should be defined analogously. Moreover, as already pointed out in [7], there is a discrepancy in the definition of the generalized Bernoulli numbers. However, the author of [7] still missed the 1/2 factor in Yu's definition (1) of generalized Bernoulli numbers.

Yu's formula can be slightly simplified.

Theorem A'. *Let all the notations be given as in Theorem A. For a prime divisor p of N, we let f_p denote the multiplicative order of p in $(\mathbb{Z}/(N/p^{n(p)})\mathbb{Z})^\times / \pm 1$, and $e_p = |(\mathbb{Z}/(N/p^{n(p)})\mathbb{Z})^\times / \pm 1|/f_p$. Then the class number $h_1^\infty(N)$ is equal to*

$$(8) \qquad h_1^\infty(N) = \prod_{p|N} \frac{p^{L(p)}(1 + p^{f_p})^{e_p}}{(1 + p)} \cdot \prod_{\chi \neq \chi_0 \ even} \frac{1}{4} B_{2,\chi},$$

where the last product is taken over all even non-principal Dirichlet characters modulo N.

Proof. We first determine the relation between $B_{2,\chi}$ and B_{2,χ_f} for a character of conductor f. We have, by the exclusion-inclusion principle,

$$B_{2,\chi} = N \sum_{a=1}^{N} B_2(a/N)\chi(a) = N \sum_{k|(N/f), \ (k,f)=1} \mu(k) \sum_{a=1}^{N/k} B_2(ak/N)\chi_f(ak).$$

The inner sum is equal to

$$\chi_f(k) \sum_{a=0}^{f-1} \chi_f(a) \sum_{m=0}^{N/(kf)-1} \left(\frac{(mf+a)^2 k^2}{N^2} - \frac{(mf+a)k}{N} + \frac{1}{6} \right)$$

$$= \chi_f(k) \sum_{a=0}^{f-1} \frac{kf}{N} B_2(a/f) \chi_f(a) = \frac{k}{N} \chi_f(k) B_{2,\chi_f}.$$

It follows that

(9) $$B_{2,\chi} = B_{2,\chi_f} \sum_{k|(N/f),\ (k,f)=1} \mu(k)\chi_f(k)k = B_{2,\chi_f} \prod_{p|N,\ p\nmid f} (1 - \chi_f(p)p),$$

and consequently,

$$h_1^\infty(N) = \prod_{p|N} p^{L(p)} \prod_{\chi \neq \chi_0} \frac{1}{4} B_{2,\chi} \prod_p \frac{1 - \chi_f(p)p^2}{1 - \chi_f(p)p}.$$

Now for each prime factor p of N, there are precisely $|(\mathbb{Z}/(N/p^{n(p)})\mathbb{Z})^\times/\pm 1|$ even Dirichlet characters modulo N whose conductors are relatively prime to p. As χ runs over such characters, the values of $\chi(p)$ go through the complete set of f_pth roots of unity e_p times. Therefore, for $a = 1,\ 2$,

$$\prod_{\chi \neq \chi_0} (1 - \chi_f(p)p^a) = \frac{(1 - p^{af_p})^{e_p}}{1 - p^a},$$

and (8) follows.   □

We now describe our method for prime power cases. Let $N = p^n$ be a prime power greater than 4, and set $n = \phi(N)/2$. The divisor group $\mathscr{D}_1^\infty(N)$ can be naturally embedded in the hyperplane $x_1 + \cdots + x_n = 0$ inside $\mathbb{R}^n$ by sending a divisor $\sum c_n(P_n)$ of degree 0 to $(c_1, \ldots, c_n)$, where P_i denote the cusps in $C_1^\infty(N)$. It is obvious that the image of $\mathscr{D}_1^\infty(N)$ is the lattice Λ generated by $V = \{(0, \ldots, 0, 1, -1, 0, \ldots, 0)\}$. Now if $f_1, \ldots, f_{n-1}$ are multiplicatively independent modular units contained in $\mathscr{F}_1^\infty(N)$, then the images of the divisors of f_i will generate a sublattice Λ' of Λ of the same rank whose index in Λ can be determined using the following lemma.

Lemma 6. *Let $\Lambda \subset \mathbb{R}^n$ be the lattice of dimension $n-1$ generated by the vectors of the form $(0, \ldots, 1, -1, 0, \ldots, 0)$. Let Λ' be a sublattice of Λ of the same rank generated by $v_1, \ldots, v_{n-1} \in \Lambda$. Let $v_n = (c_1, \ldots, c_n)$ be any vector such that $\sum_i c_i \neq 0$, and M be the $n \times n$ matrix whose ith row is v_i. Then we have*

$$(\Lambda : \Lambda') = \left| \left(\sum_{i=1}^n c_i \right)^{-1} \det M \right|.$$

Proof. In general, to determine the index of a sublattice Λ' in a lattice Λ of codimension 1 in $\mathbb{R}^n$, we pick a nonzero vector v in $\mathbb{R}^n$ that is orthogonal to Λ, and form two matrices A and A', where the rows of A are genenerators of Λ and v, while those of A' are generators of Λ' and v. Then the index of Λ' in Λ is equal to $|\det A'/\det A|$.

Now for the lattice Λ generated by $(0, \ldots, 1, -1, 0, \ldots, 0)$, we can choose the vector v to be $(1/n, \ldots, 1/n)$. Then the determinant of A is 1. On the other hand,

for the matrix M in the lemma, by adding suitable multiples of the first $n-1$ rows to the last row, we can bring the last row into $(0, \ldots, 0, c)$. Since the sum of entries in each of the first $n-1$ rows is 0, the number c is equal to the sum $\sum_i c_i$. Note that this procedure does not change the determinant. By the same token, we can also transform the matrix A' corresponding to Λ' into a matrix whose first $n-1$ rows are v_i and whose last row is $(0, \ldots, 0, 1)$ without change the determinant. From this, we see that $\det M = c \det A'$, and therefore $(\Lambda : \Lambda') = |c^{-1} \det M|$. $\qquad\square$

Now let us consider the prime case $N = p$ for the moment. Assume that $f_i(\tau) = \prod_j E_j^{e_{i,j}}$, $i = 1, \ldots, (p-1)/2 - 1$, are multiplicatively independent modular units in $\mathscr{F}_1^\infty(p)$. Let M be the square matrix of size $(p-1)/2$ whose (j, k)-entry is the order of E_j at k/p, and $U = (u_{ij})$ be the square matrix of the same size with

$$(10) \qquad u_{ij} = \begin{cases} e_{i,j}, & \text{if } 1 \le i \le (p-3)/2, \\ 0, & \text{if } i = (p-1)/2 \text{ and } 1 \le j \le (p-3)/2, \\ 1, & \text{if } i = j = (p-1)/2. \end{cases}$$

Then the product UM will have the orders of f_i at k/p as its (i, k)-entry for the first $(p-3)/2$ rows and the last row consists of the orders of $E_{(p-1)/2}$ at k/p, which, by Proposition 3 are $pB_2(k(p-1)/p)/2$. Thus, by Lemma 6, the subgroup generated by the divisors of f_i will have index

$$\left| \left(\frac{p}{2} \sum_{k=1}^{(p-1)/2} B_2\left(\frac{k(p-1)}{p}\right) \right)^{-1} \det U \det M \right|$$

in the full divisor group. In particular, $\{f_i\}$ generates $\mathscr{F}_1^\infty(p)$ if and only if this number is equal to $h_1^\infty(p)$.

By the definition of generalized Bernoulli numbers, we have

$$\frac{p}{2} \sum_{k=1}^{(p-1)/2} B_2\left(\frac{k(p-1)}{p}\right) = \frac{1}{4} B_{2,\chi_0}.$$

We now determine $\det M$, which turns out to be essentially the product of generalized Bernoulli numbers appearing in Theorem A.

Lemma 7. *Let $N \ge 4$ be an integer, $n = \phi(N)/2$, and*

$$S = \{a_i : i = 1, \ldots, n, \ 1 \le a_i \le N/2, \ (a_i, N) = 1\}.$$

For an integer b relatively prime to N, denote by b^{-1} its multiplicative inverse modulo N. Let M be the $n \times n$ matrix whose (i, j)-entry is $N B_2(a_i a_j^{-1}/N)/2$. Then we have

$$\det M = \prod_\chi \frac{1}{4} B_{2,\chi},$$

where χ runs over all even characters modulo N.

Proof. The proof is standard. We let V be the vector space over $\mathbb{C}$ of all $\mathbb{C}$-valued functions f on $(\mathbb{Z}/N\mathbb{Z})^\times$ satisfying $f(a) = f(-a)$ for all $a \in (\mathbb{Z}/N\mathbb{Z})^\times$. There are two standard bases for V. One is $\{\delta_a : a \in S\}$, where

$$\delta_a(x) = \begin{cases} 1, & \text{if } x = \pm a, \\ 0, & \text{else,} \end{cases}$$

and the other is $\{$ all even Dirichlet characters modulo $N\}$. For $a \in (\mathbb{Z}/N\mathbb{Z})^{\times}$, define $T_a : V \to V$ by $T_a f(x) = f(ax)$. Then T_a is a linear operator on V. Consider

$$T = \sum_{a \in S} \frac{N}{2} B_2(a/N) T_a.$$

We have

$$T\delta_b(x) = \sum_{a \in S} \frac{N}{2} B_2(a/N) \delta_b(ax) = \sum_{a \in S} \frac{N}{2} B_2(a/N) \delta_{a^{-1}b}(x),$$

and hence

$$T\delta_b = \sum_{c \in S} \frac{N}{2} B_2(bc^{-1}/N) \delta_c.$$

We find that the matrix of T with respect to the first basis is M.

On the other hand, we also have, for an even Dirichlet character χ modulo N,

$$T\chi(x) = \sum_{a \in S} \frac{N}{2} B_2(a/N)\chi(ax) = \sum_{a \in S} \frac{N}{2} B_2(a/N)\chi(a)\chi(x) = \frac{1}{4} B_{2,\chi}\chi(x).$$

From this we see that the matrix of T with respect to the second basis is diagonal and its determinant is the product

$$\prod_{\chi} \frac{1}{4} B_{2,\chi}$$

of eigenvalues, which equals to the determinant of M. This proves the lemma. $\square$

In summary, in the case $N = p$ is an odd prime, if $e_{i,j}$, $i = 1, \ldots, (p-3)/2$, $j = 1, \ldots, (p-1)/2$, are integers such that

$$\sum_{j=1}^{(p-1)/2} e_{i,j} = 0, \qquad \sum_{j=1}^{(p-1)/2} j^2 e_{i,j} \equiv 0 \mod p,$$

and the square matrix $U = (u_{ij})$ of size $(p-1)/2$ defined by (10) has determinant p, then according to Theorem A, $f_i = \prod_j E_j^{e_{i,j}}$, $i = 1, \ldots, (p-3)/2$, form a basis for $\mathscr{F}_1^{\infty}(p)$.

For prime power cases $N = p^n$, the basic idea is similar. We pick a generator a of $(\mathbb{Z}/p^n\mathbb{Z})^{\times}/\pm 1$ and form a $\phi(N)/2 \times \phi(N)/2$ matrix M with the (i,j)-entry being the order of $E_{a^{i-1}}$ at a^{j-1}/N. Then we try to find another $\phi(N)/2 \times \phi(N)/2$ matrix U such that

(1) the first $\phi(N)/2 - 1$ rows of UM has the interpretation as the orders of some functions in $\mathscr{F}_1^{\infty}(N)$,
(2) the last row of U is $(0, \ldots, 0, 1)$,
(3) the determinant of U equals to $p^{L(p)}$.

However, unlike the prime cases, the functions E_g with $(g, N) = 1$ will not be sufficient to generate the whole group $\mathscr{F}_1^{\infty}(N)$ and it is necessary to use functions from lower level, i.e., functions of the form $E_g^{(p^{\ell})}(p^{n-\ell}\tau) = E_{gp^{n-\ell}}^{(N)}(\tau)$ for some $\ell < n$. To record the orders of such a function at cusps, we will invoke the distribution relation (6) in Lemma 5. We leave the details to Section 3.2.

2.4. **Method for non-prime power cases.** In this section, we explain our idea for non-prime power cases.

In theory, it is still possible to use the same method as the prime power cases, but the argument will become extremely tedious. Thus, instead of using Theorem A and the linear algebra argument, we use the following characterization of $\mathscr{F}_1^\infty(N)$ of Yu [31].

Theorem B (Yu, [31, Lemma 2.1 and Theorem 4]). *Let N be a positive integer having at least two distinct prime divisors. Then, up to a scalar, $f(\tau)$ belongs to $\mathscr{F}_1^\infty(N)$ if and only if $f(\tau) = \prod_g E_g^{e_g}$ is a product of E_g satisfying*

$$(11) \qquad \sum_{g \in \mathcal{O}_{a,p}} e_g = 0$$

for each prime divisor p of N and each $a \in \mathbb{Z}/N\mathbb{Z}$.

Our idea is perhaps best explained by giving an example.

Example. Consider $N = 21$. Assume that $f(\tau) = \prod_{g=1}^{10} E_g^{e_g}$ is a modular unit in $\mathscr{F}_1^\infty(21)$. Then the orbit condition (11) gives

$$e_7 = 0, \quad e_3 = -e_4 - e_{10}, \quad e_6 = -e_1 - e_8, \quad e_9 = -e_2 - e_5,$$

and

$$e_1 + e_2 + e_4 + e_5 + e_8 + e_{10} = 0.$$

Then we have

$$f = \left(\frac{E_1}{E_6}\right)^{e_1} \left(\frac{E_2}{E_9}\right)^{e_2} \left(\frac{E_4}{E_3}\right)^{e_4} \left(\frac{E_5}{E_9}\right)^{e_5} \left(\frac{E_8}{E_6}\right)^{e_8} \left(\frac{E_{10}}{E_3}\right)^{e_{10}},$$

subject to the condition $e_1 + e_2 + e_4 + e_5 + e_8 + e_{10} = 0$. Thus, if we let F_i, $i = 1, 2, 4, 5, 8, 10$, denote the 6 quotients in the last expression, then F_1/F_2, F_2/F_4, F_4/F_5, F_5/F_8, F_8/F_{10} will generate $\mathscr{F}_1^\infty(21)$.

The above example shows that for a squarefree composite integer N, we may regard any $\phi(N)/2 - 1$ exponents e_g from the set $\{e_g : 1 \le g \le N/2, (g, N) = 1\}$ as "free variables" and express the rest of e_g in terms of these free variables. This gives a basis for $\mathscr{F}_1^\infty(N)$.

When N is not squarefree, the situation is much more complicated as there are relations among $\{e_g : 1 \le g \le N/2, (g, N) = 1\}$ other than $\sum_{(g,N)=1} e_g = 0$. For instance, when $N = 63$, the orbit conditions include $e_1 + e_{22} + e_{20} = 0$, $e_2 + e_{23} + e_{19} = 0$, and so on. (The situation is reminiscent of the case of cyclotomic units where non-trivial relations exist among the units $1 - e^{2\pi i k/N}$.) Then, again, modular units from modular curves of lower levels are needed to obtain a basis for $\mathscr{F}_1^\infty(N)$. We leave the details to Section 4.

3. Prime power cases

3.1. **Prime cases.** In this section, we consider the simplest case when the level is a prime.

Theorem 1. *Let $N = p$ be an odd prime greater than 3. Let a be a generator of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times / \pm 1$ and b be its multiplicative inverse modulo p. Let*

$n = (p-1)/2$. *Then the functions*

$$\frac{E_{a^{i-1}}E_{a^{i+1}}^{b^2}}{E_{a^i}^{1+b^2}}, \quad i = 1,\ldots,n-2, \quad and \quad \frac{E_{b^2}^p}{E_b^p}$$

generate $\mathscr{F}_1^\infty(p)$ modulo $\mathbb{C}^\times$.

Proof. Let p, a, b, and n be given as in the statement. There are n essentially distinct E_g, and there are n cusps k/p, $k = 1,\ldots,n$, of $X_1(p)$ that are lying over ∞ of $X_0(p)$. By Proposition 3, the order of E_g at k/p is $pB_2(gk/p)/2$. We form an $n \times n$ matrix $M = (M_{ij})$ by setting

$$M_{ij} = \frac{p}{2}B_2(a^{i+j-2}/p)$$

to be the order of $E_{a^{i-1}}$ at a^{j-1}/p. Set

(12)
$$U_1 = \begin{pmatrix} 1 & -b^2 & 0 & \cdots & \cdots & \cdots \\ 0 & 1 & -b^2 & \cdots & \cdots & \cdots \\ \vdots & \vdots & & & \vdots & \vdots \\ \cdots & \cdots & \cdots & 0 & 1 & -b^2 \\ \cdots & \cdots & \cdots & 0 & 0 & 1-b^2 \end{pmatrix}.$$

In other words, U_1 has $-b^2$ on the superdiagonal and 1 on the diagonal, except for the last one, which has $1 - b^2$. Note that for $i = 1,\ldots,n-1$, the ith row of the matrix U_1M now records the orders of $E_{a^{i-1}}/E_{a^i}^{b^2}$ at cusps.

Furthermore, set

(13)
$$U_2 = \begin{pmatrix} 1 & -1 & 0 & \cdots & \cdots & \cdots \\ 0 & 1 & -1 & \cdots & \cdots & \cdots \\ \vdots & \vdots & & & \vdots & \vdots \\ \cdots & \cdots & \cdots & 1 & -1 & 0 \\ \cdots & \cdots & \cdots & 0 & p & -p \\ \cdots & \cdots & \cdots & 0 & 0 & 1 \end{pmatrix}$$

The matrix U_2 has -1 on the superdiagonal and 1 on the diagonal, except for the $(n-1)$-st row, which has $-p$ and p, respectively. Then the first $n-2$ rows of the matrix U_2U_1M describe the orders of $f_i = E_{a^{i-1}}E_{a^{i+1}}^{b^2}/E_{a^i}^{1+b^2}$ at cusps. Also, the $(n-1)$-st row gives the orders of $f_{n-1} = E_{b^2}^p/E_b^p$ at cusps. By Proposition 2, these functions are all modular on $\Gamma_1(p)$. Moreover, by Proposition 3, f_i has no poles nor zeros at cusps that are not of the form k/p. Thus, the functions f_i belong to the group $\mathscr{F}_1^\infty(p)$. We will show that these functions are a basis of $\mathscr{F}_1^\infty(p)$ modulo $\mathbb{C}^\times$, or equivalently, that the divisors of these functions f_i form a $\mathbb{Z}$-basis for the additive group $\operatorname{div}\mathscr{F}_1^\infty(p)$.

It is obvious that the divisor group $\mathscr{D}_1^\infty(p)$ is generated by $(1/p)-(a/p)$, $(a/p)-(a^2/p)$, $\cdots$, $(b^2/p)-(b/p)$. Thus, according to Lemma 6, the index of the subgroup generated by the divisors of f_i in the group $\mathscr{D}_1^\infty(p)$ is the absolute value of $\det(U_2U_1M)$ divided by the sum of the entries in the last row of U_2U_1M. It remains to show that it has the correct value as given in (7).

By Lemma 7, the determinant of M is, up to ± 1 sign,

$$\det M = \prod_\chi \frac{1}{4}B_{2,\chi}$$

(Note that the matrix M here differs from the one in Lemma 7 by multiplication by permutation matrices on the two sides.) Also, the determinants of U_1 and U_2 are $1 - b^2$ and p, respectively. Now the last row of $U_2 U_1$ is $(0, \ldots, 0, 1 - b^2)$. If follows that the sum of the entries in the last row of $U_2 U_1 M$ is equal to

$$(1 - b^2) \sum_{k=1}^{(p-1)/2} \frac{p}{2} B_2(k/p) = \frac{1 - b^2}{4} B_{2,\chi_0}.$$

and the index is equal to the absolute value of

$$\frac{4}{(1 - b^2) B_{2,\chi_0}} \det(U_2 U_1 M) = \frac{4}{(1 - b^2) B_{2,\chi_0}} \cdot p \cdot (1 - b^2) \prod_{\chi} \frac{1}{4} B_{2,\chi} = p \prod_{\chi \neq \chi_0} \frac{1}{4} B_{2,\chi},$$

which is indeed the index of $\operatorname{div} \mathscr{F}_1^\infty(p)$ in $\mathscr{D}_1^\infty(p)$. In other words, the functions f_i form a basis for $\mathscr{F}_1^\infty(p)$ modulo $\mathbb{C}^\times$. This completes the proof of the theorem. $\square$

We now give an example demonstrating our idea.

Example. Let $N = 13$. We choose the generator a of the group $(\mathbb{Z}/13\mathbb{Z})^\times$ to be $a = 7$. Then the multiplicative inverse of a modulo 13 is $b = 2$. The cusps of $X_1(13)$ lying over ∞ of $X_0(13)$ are $i/13$, $i = 1, \ldots, 6$. We denote these cusps by $P_i = a^{i-1}/13$, $i = 1, \ldots, 6$. Then the matrix M is

$$M = (13 B_2(7^{i+j-2}/13)/2)_{ij} = \frac{1}{156} \begin{pmatrix} 97 & -83 & -11 & -71 & -47 & 37 \\ -83 & -11 & -71 & -47 & 37 & 97 \\ -11 & -71 & -47 & 37 & 97 & -83 \\ -71 & -47 & 37 & 97 & -83 & -11 \\ -47 & 37 & 97 & -83 & -11 & -71 \\ 37 & 97 & -83 & -11 & -71 & -47 \end{pmatrix}.$$

With U_1 and U_2 given by (12) and (13), we find

$$U_2 U_1 M = \begin{pmatrix} 3 & -2 & 1 & 2 & 1 & -5 \\ -2 & 1 & 2 & 1 & -5 & 3 \\ 1 & 2 & 1 & -5 & 3 & -2 \\ 2 & 1 & -5 & 3 & -2 & 1 \\ -7 & -5 & 15 & -6 & 5 & -2 \\ c_1 & c_2 & c_3 & c_4 & c_5 & c_6 \end{pmatrix},$$

where $(c_1, \ldots, c_6)$ is -3 times the last row of M. The first 5 rows represent the orders of $f_1 = E_1 E_3^4 / E_6^5$, $f_2 = E_6 E_5^4 / E_3^5$, $f_3 = E_3 E_4^4 / E_5^5$, $f_4 = E_5 E_2^4 / E_4^5$, and E_4^{13}/E_2^{13} at the cusps P_j, respectively. Since the determinant of $U_2 U_1 M$ is $57/2$ and the sum of c_i is $3/2$, according to Lemma 6, we find the index of the subgroup generated by the divisors of f_i in $\mathscr{D}_1^\infty(13)$ is 19, which agrees with the divisor class number obtained from (7). In other words, f_i generate $\mathscr{F}_1^\infty(13)$.

Now observe that the divisor class group $\mathscr{D}_1^\infty(13)/\operatorname{div} \mathscr{F}_1(13)$ is cyclic. Thus, there is an integer m with $0 < m < 19$ such that $m(P_1) - m(P_2)$ and $(P_2) - (P_3)$ are in the same class, i.e., $m(P_1) - (m+1)(P_2) + (P_3)$ is a principal divisor. This integer m has the property that the equation

$$(c_1, c_2, c_3, c_4, c_5, c_6) U_3 U_2 U_1 M = (m, -m - 1, 1, 0, 0, 0)$$

has an integer solution. We find that this occurs when $m = 8$ with

$$(c_1, \ldots, c_6) = (9, 40, 167, 675, 208, 0).$$

This integer m also satisfies $m(P_2) - m(P_3) \sim (P_3) - (P_4)$, $m(P_3) - m(P_4) \sim (P_4) - (P_5)$, and so on. This is because if $f(\tau)$ is a modular function on $\Gamma_1(13)$ such that

$$\operatorname{div} f = m(P_1) - (m+1)(P_2) + (P_3),$$

then

$$\operatorname{div} f \Big| \begin{pmatrix} 6 & -2 \\ 13 & -1 \end{pmatrix} = m(P_2) - (m+1)(P_3) + (P_4),$$

$$\operatorname{div} f \Big| \begin{pmatrix} 6 & -2 \\ 13 & -1 \end{pmatrix}^2 = m(P_3) - (m+1)(P_4) + (P_5),$$

and so on. From these informations, we see that the divisor

$$\sum_{i=1}^{6} d_i (P_i)$$

and

$$\{d_1 + 8(d_1 + d_2) + 8^2(d_1 + d_2 + d_3) + \cdots + 8^4(d_1 + d_2 + d_3 + d_4 + d_5)\}$$
$$\cdot ((P_1) - (P_2)) + (d_1 + d_2 + \cdots + d_6)(P_6)$$

are in the same divisor class. In particular, it is principal if and only if

$$d_1 + d_2 + \cdots + d_6 = 0, \qquad 7d_1 + 6d_2 + 17d_3 + 10d_4 + 11d_5 \equiv 0 \mod 19.$$

3.2. **Prime power cases.** In this section we deal with the cases where $N = p^k$ is a prime power. For the ease of exposition, odd prime power cases and even prime power cases are stated as two theorems, even though the proofs are very similar.

We first describe two constructions of modular functions belonging to $\mathscr{F}_1^\infty(p^k)$.

Lemma 8. *Let p be a prime, and k be an integer greater than 1. Suppose that g and e_g are integers satisfying $p \nmid g$ and*

$$\sum_g g^2 e_g \equiv 0 \mod p$$

Then

$$\prod_g \left(\frac{E_g}{E_{g(1+mp^{k-1})}} \right)^{e_g}$$

is a modular function in $\mathscr{F}_1^\infty(p^k)$ for all integers m.

Proof. It is easy to see from Proposition 2 that the functions concerned are all modular on $\Gamma_1(p^k)$. These functions also satisfy the orbit condition in Lemma 4. Thus, they are contained in $\mathscr{F}_1^\infty(p^k)$. $\qquad\square$

The second method uses functions from lower levels.

Lemma 9. *Assume that $N = pM$. If e_g are integers such that*

$$\sum_g e_g \equiv 0 \mod 12, \qquad \sum_g g e_g \equiv 0 \mod 2,$$

and

$$\sum_g g^2 e_g \equiv 0 \mod \begin{cases} 2M, & \text{if } p \nmid M, \\ 2M/p, & \text{if } p \mid M, \end{cases}$$

then $\prod_g E_g^{(M)}(p\tau)^{e_g}$ is a modular function on $\Gamma_1(N)$. Moreover, if M is odd, then the conditions can be relaxed to

$$\sum_g e_g \equiv 0 \mod 12, \qquad \sum_g g^2 e_g \equiv 0 \mod \begin{cases} M, & \text{if } p \nmid M, \\ M/p, & \text{if } p | M. \end{cases}$$

Proof. Let $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$. We have

$$(14) \qquad p\sigma\tau = p\frac{a\tau + b}{c\tau + d} = \frac{a(p\tau) + bp}{(c/p)(p\tau) + d} = \begin{pmatrix} a & bp \\ c/p & d \end{pmatrix}(p\tau).$$

Then by (3) of Proposition 1,

$$E_g^{(M)}(p\sigma\tau) = \epsilon(a, bpM, c/pM, d)e^{\pi i(g^2 abp/M - gbp)}E_{ag}^{(M)}(p\tau).$$

Then the assumptions $\sum_g e_g \equiv 0 \mod 12$ and $\sum_g g e_g \equiv 0 \mod 2$ imply that

$$\prod E_g^{(M)}(p\sigma\tau)^{e_g} = \exp\left\{\pi i abp \sum g^2 e_g / M\right\} \prod E_{ag}^{(M)}(p\tau)^{e_g}.$$

When $p \nmid M$, the condition $\sum_g g^2 e_g \equiv 0 \mod 2M$ ensures that the exponential factor is equal to 1. When $p | M$, the condition $\sum_g g^2 e_g \equiv 0 \mod 2M/p$ will suffice. In either case, we have

$$\prod E_g^{(M)}(p\sigma\tau)^{e_g} = \prod E_{ag}^{(M)}(p\tau)^{e_g}.$$

Finally, equality (2) in Proposition 1 and the assumption $\sum g e_g \equiv 0 \mod 2$ show that

$$\prod E_g^{(M)}(p\sigma\tau)^{e_g} = \prod (-1)^{g e_g (a-1)/N} E_g^{(M)}(p\tau)^{e_g} = \prod E_g^{(M)}(p\tau)^{e_g}.$$

When M is odd, since $E_g^{(M)} = E_{M-g}^{(M)}$, we may assume that all g are even so that $\sum g e_g \equiv 0$, $\sum g^2 e_g \equiv 0 \mod 2$ are always satisfied. Also, $g^2 \equiv (M-g)^2 \mod M$. Therefore, the conditions can be reduced to $\sum e_g \equiv 0 \mod 12$ and $\sum g^2 e_g \equiv 0 \mod M$ when M is odd. This completes the proof. $\qquad\square$

Lemma 10. *Let p a prime. Assume that $N = pM$. If $f(\tau)$ is a modular function on $X_1(M)$, then $f(p\tau)$ is a modular function on $X_1(N)$. Furthermore, if p also divides M and $f(\tau)$ belongs to the group $\mathscr{F}_1^\infty(M)$, then the function $f(p\tau)$ belongs to the group $\mathscr{F}_1^\infty(N)$.*

Proof. Assume that $f(\tau)$ is modular on $\Gamma_1(M)$. Given $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$, we have, by (14),

$$p\sigma\tau = \begin{pmatrix} a & bp \\ c/p & d \end{pmatrix}(p\tau).$$

Since $f(\tau)$ is assumed to be modular on $\Gamma_1(M)$, we have $f(p\sigma\tau) = f(p\tau)$. That is, $f(p\tau)$ is modular on $\Gamma_1(N)$.

Now assume that $p | M$ and $f(\tau) \in \mathscr{F}_1^\infty(M)$. The assumption that $f(\tau)$ has no zeros nor poles in $\mathbb{H}$ implies that $f(p\tau)$ has the same property. Now we check that the poles and zeros of $f(p\tau)$ occurs only at cusps lying over ∞ of $X_0(N)$.

In general, the cusps of $X_1(N)$ takes the form a/c with $c | N$ and $(a, c) = 1$. Choose integers b and d such that

$$\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z}).$$

Then the order of a modular function $g(\tau)$ on $X_1(N)$ at a/c is determined by the Fourier expansion of $g(\sigma\tau)$. In particular, $g(\tau)$ has no pole nor zero at a/c if and only if the Fourier expansion of $g(\sigma\tau)$ starts from a non-vanishing constant term.

Now a/c does not lie over ∞ of $X_0(N)$ if and only c is a proper divisor of N. We will show that $f(p\tau)$ has no poles nor zeros at such points. This amounts to proving the assertion that $\lim_{\tau\to\infty} f(p\sigma\tau)$ is finite and non-vanishing for such a/c. We consider two cases $p|c$ and $p \nmid c$ separately.

When $p|c$, we have $\lim_{\tau\to\infty} f(p\sigma\tau) = f(a/(c/p))$. Since the denominator c/p is a proper divisor of M, by assumption that $f(\tau) \in \mathscr{F}_1^\infty(M)$, $\lim_{\tau\to\infty} f(p\sigma\tau)$ is finite and non-vanishing.

When $p \nmid c$, we have $\lim_{\tau\to\infty} p\sigma\tau = pa/c$. By the assumption that $p|M$, the denominator c is a proper divisor of M. Thus, we conclude again that $f(p\tau)$ has no poles nor zeros at a/c. This completes the proof. $\qquad\square$

Combining the above two lemmas, we obtain a simple construction of modular functions that are in $\mathscr{F}_1^\infty(p^k)$.

Corollary 11. *Let p be a prime and $k \geq 2$ be a positive integer. Then*

$$E_g^{(p^\ell)}(p^{k-\ell}\tau)/E_{g+mp^{\ell-1}}^{(p^\ell)}(p^{k-\ell}\tau)$$

are all modular functions contained in $\mathscr{F}_1^\infty(p^k)$ for all $\ell = 1, \ldots, k-1$ and all g and m satisfying g, $g + mp^{\ell-1} \not\equiv 0 \mod p^\ell$.

Proof. First of all, Lemma 9 shows that $f(\tau) = E_g^{(p^\ell)}(p\tau)/E_{g+mp^{\ell-1}}^{(p^\ell)}(p\tau)$ is a modular function on $\Gamma_1(p^{\ell+1})$. Then the first part of Lemma 10 implies that $f(p^{k-\ell-1}\tau)$ is modular on $\Gamma_1(p^k)$ for all $k > \ell$. We now prove that it has poles and zeros only at cusps in $C_1^\infty(p^k)$.

Lemma 8 shows that $f(\tau/p)^p = E_g^{(p^\ell)}(\tau)^p/E_{g+mp^{\ell-1}}^{(p^\ell)}(\tau)^p$ is in $\mathscr{F}_1^\infty(p^\ell)$. Then Lemma 10 implies that $f(p^{k-\ell-1}\tau)^p$ has poles and zeros only at cusps in $C_1^\infty(p^k)$, and so is $f(p^{k-\ell-1}\tau)$. We conclude that $f(p^{k-\ell-1}\tau)$ is in $\mathscr{F}_1^\infty(p^k)$, as claimed in the statement of the lemma. $\qquad\square$

With the above lemmas we can now determine a basis for $\mathscr{F}_1^\infty(p^k)$ for odd primes p and integers $k \geq 2$.

Theorem 2. *Let $k > 1$ and $N = p^k$ be an odd prime power. For a positive integer ℓ, we set $\phi_\ell = \phi(p^\ell)/2$. Let a be a generator of the cyclic group $(\mathbb{Z}/p^k\mathbb{Z})^\times/\pm 1$ and b be its multiplicative inverse modulo p. Then a basis for $\mathscr{F}_1^\infty(p^k)$ modulo $\mathbb{C}^\times$ is*

given by

$$\begin{cases} f_i = \dfrac{E_{a^{i-1}} E_{a^{i+\phi_{k-1}}}^{b^2}}{E_{a^{i+\phi_{k-1}-1}} E_{a^i}^{b^2}}, & i = 1, \ldots, \phi_k - \phi_{k-1} - 1, \\[2mm] f_i = \dfrac{E_{a^{i-1}}^p}{E_{a^{i+\phi_{k-1}-1}}^p}, & i = \phi_k - \phi_{k-1}, \\[2mm] f_i = \dfrac{E_{a^{i-1}}^{(p^{k-1})}(p\tau)}{E_{a^{i+\phi_{k-2}-1}}^{(p^{k-1})}(p\tau)}, & i = \phi_k - \phi_{k-1} + 1, \ldots, \phi_k - \phi_{k-2}, \\[2mm] \vdots & \vdots \\[2mm] f_i = \dfrac{E_{a^{i-1}}^{(p^2)}(p^{k-2}\tau)}{E_{a^{i+\phi_1-1}}^{(p^2)}(p^{k-2}\tau)}, & i = \phi_k - \phi_2 + 1, \ldots, \phi_k - \phi_1, \\[2mm] f_i = \dfrac{E_{a^{i-1}}^{(p)}(p^{k-1}\tau)}{E_{a^i}^{(p)}(p^{k-1}\tau)}, & i = \phi_k - \phi_1 + 1, \ldots, \phi_k - 1. \end{cases}$$

Proof. Form a $\phi_k \times \phi_k$ matrix $M = (M_{ij})$, where

$$M_{ij} = \frac{p^k}{2} B_2\left(\frac{a^{i+j-2}}{p^k}\right).$$

In other words, M_{ij} is the order of $E_{a^{i-1}}$ at a^{j-1}/p^k. For $\ell = 2, \ldots, k$, define a $\phi_\ell \times \phi_\ell$ matrix V_ℓ by

(15)
$$V_\ell = \begin{pmatrix} I & -I & 0 & \cdots & \cdots & \cdots \\ 0 & I & -I & \cdots & \cdots & \cdots \\ \vdots & \vdots & & & \vdots & \vdots \\ \cdots & \cdots & \cdots & I & -I & 0 \\ \cdots & \cdots & \cdots & 0 & I & -I \\ pI & pI & \cdots & \cdots & pI & pI \end{pmatrix}.$$

Here the matrix consists of p^2 blocks, each of which is of $\phi_{\ell-1} \times \phi_{\ell-1}$ size, and I is the identity matrix, while 0 is the zero matrix. Define also $\phi_k \times \phi_k$ matrices U_ℓ, $\ell = 1, \ldots, k$, by

(16)
$$U_k = V_k$$

and for $\ell = 2, \ldots, k-1$,

(17)
$$U_\ell = \begin{pmatrix} I & 0 & 0 & \cdots & \cdots & \cdots \\ 0 & I & 0 & \cdots & \cdots & \cdots \\ \vdots & \vdots & & & \vdots & \vdots \\ \cdots & \cdots & \cdots & I & 0 & 0 \\ \cdots & \cdots & \cdots & 0 & I & 0 \\ 0 & 0 & \cdots & \cdots & 0 & V_\ell \end{pmatrix}.$$

In other words, U_ℓ is obtained by replacing the lower right $\phi_\ell \times \phi_\ell$ block of an $\phi_k \times \phi_k$ identity matrix by V_ℓ. Also, define U_1 to be

$$U_1 = \begin{pmatrix} I & 0 & 0 & \cdots & \cdots & \cdots \\ 0 & 1 & -1 & 0 & 0 & \cdots \\ 0 & 0 & 1 & -1 & 0 & \cdots \\ \vdots & \vdots & & & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & 1 & -1 \\ 0 & 0 & \cdots & \cdots & 0 & 1 \end{pmatrix},$$

where the identity block in the upper left corner is of size $\phi_k - \phi_1$. Finally, let b be the multiplicative inverse of a modulo p and define U_k' by

$$
(18) \qquad U_k' = \begin{pmatrix}
1 & -b^2 & 0 & \cdots & \cdots & \cdots \\
0 & 1 & -b^2 & \cdots & \cdots & \cdots \\
\vdots & \vdots & & & \vdots & \vdots \\
\cdots & \cdots & \cdots & 1 & -b^2 & 0 \\
\cdots & \cdots & \cdots & 0 & p & 0 \\
0 & 0 & \cdots & \cdots & 0 & I
\end{pmatrix}
$$

where the I in the lower right corner is the identity matrix of size ϕ_{k-1}, and the diagonals are all 1 except for the row just above I. Also, the $(i, i+1)$-entries are $-b^2$ for $i = 1, \ldots, \phi_k - \phi_{k-1} - 1$. Now let us consider the effect of the multiplication of M by $U_1 U_2 \ldots U_{k-1} U_k' U_k$ on the left. We will show that the first $\phi_k - 1$ rows of the resulting matrix will be a basis for the lattice corresponding to div $\mathscr{F}_1^\infty(p^k)$.

Clearly, the first $\phi_k - \phi_{k-1}$ rows of $U_k M$ record the orders of the functions $E_{a^{i-1}}^{(p^k)}/E_{a^{i+\phi_{k-1}-1}}^{(p^k)}$. The entries in the last few rows of $U_k M$ take the form

$$
p \sum_{m=0}^{p-1} \frac{p^k}{2} B_2 \left(\frac{a^{i+j+m\phi_{k-1}-2}}{p^k} \right).
$$

Now observe that as m runs through 0 to $p-1$, $a^{m\phi_{k-1}}$ modulo p^k goes through exactly once elements of $\{1 + \ell p^{k-1} : \ell = 0, \ldots, p-1\}$ modulo ± 1. (Note that since a is a generator of $(\mathbb{Z}/p^k\mathbb{Z})^\times$, $a^{(p-1)/2} = -1 + \ell p$ for some ℓ not divisible by p. Then $a^{\phi_{k-1}} = (-1+\ell p)^{p^{k-2}} \equiv -1 + \ell p^{k-1} \mod p^k$.) Then by the relation between generalized Bernoulli numbers given in Lemma 5, the above sum is equal to

$$
p \cdot \frac{p^{k-1}}{2} B_2 \left(\frac{a^{i+j-2}}{p^{k-1}} \right),
$$

which we can interpret as the order of $E_{a^{i-1}}^{(p^{k-1})}(p\tau)$ at cusps a^{j-1}/p^k.

Then the first $\phi_k - \phi_{k-1} - 1$ rows of $U_k' U_k M$ will be the orders of

$$
f_i = \frac{E_{a^{i-1}} E_{a^{i+\phi_{k-1}}}^{b^2}}{E_{a^{i+\phi_{k-1}-1}} E_{a^i}^{b^2}}, \qquad i = 1, \ldots, \phi_k - \phi_{k-1} - 1,
$$

at cusps. Also, the $(\phi_k - \phi_{k-1})$-th row of $U_k' U_k M$ corresponds to the function

$$
f_{\phi_k - \phi_{k-1}} = \frac{E_{a^{\phi_k - \phi_{k-1}-1}}^p}{E_{a^{\phi_k-1}}^p}.
$$

Since $a^{\phi_{k-1}} = a^{p^{k-2}(p-1)/2} \equiv \pm 1 \mod p^{k-1}$, by Lemma 8, these functions f_i are all in $\mathscr{F}_1^\infty(p^k)$. Summarizing, we find that the rows of $U_k' U_k M$ record the orders of the functions

$$
f_1, \ldots, f_{\phi_k - \phi_{k-1}}, E_1^{(p^{k-1})}(p\tau), E_{a^{\phi_k - \phi_{k-1}}}^{(p^{k-1})}(p\tau), \ldots, E_{a^{\phi_k-1}}^{(p^{k-1})}(p\tau)
$$

at cusps in $C_1^\infty(p^k)$.

Now consider $U_{k-1}U_k'U_kM$. The multiplication of U_{k-1} on the left leaves the first $\phi_k - \phi_{k-1}$ rows invariant. The next $\phi_{k-1} - \phi_{k-2}$ rows now record the order of

$$f_i = \frac{E_{a^{i-1}}^{(p^{k-1})}(p\tau)}{E_{a^{i+\phi_{k-2}-1}}^{(p^{k-1})}(p\tau)}, \qquad i = \phi_k - \phi_{k-1} + 1, \ldots, \phi_k - \phi_{k-2},$$

which, by Corollary 11, are all modular functions contained in $\mathscr{F}_1^\infty(p^k)$. Also, the last ϕ_{k-2} rows of $U_{k-1}U_k'U_kM$ now have

$$p^2 \sum_{m=0}^{p-1} \frac{p^{k-1}}{2} B_2\left(\frac{a^{i+j+m\phi_{k-2}-2}}{p^{k-1}}\right)$$

as entries. By Lemma 5, the above sum is equal to

$$p^2 \cdot \frac{p^{k-2}}{2} B_2\left(\frac{a^{i+j-2}}{p^{k-2}}\right).$$

This number is precisely the order of $E_{a^{i-1}}^{(p^{k-2})}(p^2\tau)$ at a^{j-1}/p^k.

Continuing in the same way, we find that the rows of $U_1 U_2 \ldots U_{k-1} U_k' U_k M$ represent the orders of the functions

$$\begin{cases} f_i = \dfrac{E_{a^{i-1}} E_{a^{i+\phi_{k-1}}}^{b^2}}{E_{a^{i+\phi_{k-1}-1}} E_{a^i}^{b^2}}, & i = 1, \ldots, \phi_k - \phi_{k-1} - 1, \\[2mm] f_i = \dfrac{E_{a^{i-1}}^{p}}{E_{a^{i+\phi_{k-1}-1}}^{p}}, & i = \phi_k - \phi_{k-1}, \\[2mm] f_i = \dfrac{E_{a^{i-1}}^{(p^{k-1})}(p\tau)}{E_{a^{i+\phi_{k-2}-1}}^{(p^{k-1})}(p\tau)}, & i = \phi_k - \phi_{k-1} + 1, \ldots, \phi_k - \phi_{k-2}, \\[2mm] \quad\vdots & \quad\vdots \\[2mm] f_i = \dfrac{E_{a^{i-1}}^{(p^2)}(p^{k-2}\tau)}{E_{a^{i+\phi_1-1}}^{(p^2)}(p^{k-2}\tau)}, & i = \phi_k - \phi_2 + 1, \ldots, \phi_k - \phi_1, \\[2mm] f_i = \dfrac{E_{a^{i-1}}^{(p)}(p^{k-1}\tau)}{E_{a^i}^{(p)}(p^{k-1}\tau)}, & i = \phi_k - \phi_1 + 1, \ldots, \phi_k - 1, \\[2mm] E_{a^{i-1}}^{(p)}(p^{k-1}\tau), & i = \phi_k. \end{cases}$$

Except for the last one, the functions are all modular functions belonging to $\mathscr{F}_1^\infty(p^k)$. We now prove that these functions form a basis for $\mathscr{F}_1^\infty(p^k)$ modulo $\mathbb{C}^\times$. In view of Lemma 6, we need to show that the absolute value of the determinant of $U_1 \ldots U_{k-1} U_k' U_k M$ divided by the sum of the entries in its last row is equal to $h_1^\infty(p^k)$.

We first determine the sum of the entries in the last row of $U_1 \ldots U_{k-1} U_k' U_k M$. Let w denote the sequence $1, 0, \ldots, 0$, of length $(p-1)/2$, where the first number is 1 and the rest are 0. Then inductively, we can show that the last row of $U_1 \ldots U_\ell$ is $(0, \ldots, 0, p^{\ell-1}w, \ldots, p^{\ell-1}w)$ for $1 < \ell < k$, where there are $p^{\ell-1}$ copies of $p^{\ell-1}w$ at the end of the row with the preceding entries all being 0. The multiplication on the right by U_k' does not change the last row of $U_1 \ldots U_{k-1}$. Then we find the last row of $U_1 \ldots U_{k-1} U_k' U_k$ is $(p^{k-1}w, \ldots, p^{k-1}w) = (p^{k-1}, 0, \ldots, 0, p^{k-1}, \ldots)$, where there are $(p-3)/2$ zeros between two p^{k-1}. Thus, the sum of the entries in the last row of $U_1 \ldots U_{k-1} U_k' U_k M$ is

$$p^{2k-2} \sum_{j \le p^k/2,\, p\nmid j} \frac{p^k}{2} B_2(j/p^k) = \frac{p^{2k-2}}{4} B_{2,\chi_0}.$$

Now we have $\det U_1 = 1$, $\det U_k' = p$, and $\det U_\ell = p^{2\phi_{\ell-1}}$ for $\ell = 2, \ldots, k$. Also, by Lemma 7, up to a ± 1 sign,

$$\det M = \prod_\chi \frac{1}{4} B_{2,\chi}$$

Thus, the index is equal to the absolute value of

$$\frac{4}{p^{2k-2} B_{2,\chi_0}} \cdot p^{2(\phi_1 + \phi_2 + \cdots + \phi_{k-1})} \cdot p \cdot \prod_\chi \frac{1}{4} B_{2,\chi} = p^{p^{k-1} - 2k + 2} \prod_{\chi \neq \chi_0} \frac{1}{4} B_{2,\chi}.$$

This is exactly the class number given in Yu's formula. In other words, f_1, $i = 1, \ldots, \phi_k - 1$, generate $\mathscr{F}_1^\infty(p^k)$. This completes the proof. $\square$

Example. Consider $N = 27$. A generator of $(\mathbb{Z}/27\mathbb{Z})^\times$ is 2. With the notations as above, we have

$$M = \frac{1}{108} \begin{pmatrix} 191 & 143 & 59 & -61 & -109 & 23 & -97 & -37 & -121 \\ 143 & 59 & -61 & -109 & 23 & -97 & -37 & -121 & 191 \\ 59 & -61 & -109 & 23 & -97 & -37 & -121 & 191 & 143 \\ -61 & -109 & 23 & -97 & -37 & -121 & 191 & 143 & 59 \\ -109 & 23 & -97 & -37 & -121 & 191 & 143 & 59 & -61 \\ 23 & -97 & -37 & -121 & 191 & 143 & 59 & -61 & -109 \\ -97 & -37 & -121 & 191 & 143 & 59 & -61 & -109 & 23 \\ -37 & -121 & 191 & 143 & 59 & -61 & -109 & 23 & -97 \\ -121 & 191 & 143 & 59 & -61 & -109 & 23 & -97 & -37 \end{pmatrix},$$

where the (i,j)-entry is $27 B_2(2^{i+j-2}/27)/2$, U_1 is equal to the identity matrix,

$$U_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 3 & 3 \end{pmatrix}, \qquad U_3 = \begin{pmatrix} 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 \\ 3 & 0 & 0 & 3 & 0 & 0 & 3 & 0 & 0 \\ 0 & 3 & 0 & 0 & 3 & 0 & 0 & 3 & 0 \\ 0 & 0 & 3 & 0 & 0 & 3 & 0 & 0 & 3 \end{pmatrix},$$

and

$$U_3' = \begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then setting $Q = U_1 U_2 U_3' U_3 M$, we have

$$Q = \begin{pmatrix} 0 & 2 & 0 & 1 & -2 & 4 & -1 & 0 & -4 \\ 2 & 0 & 1 & -2 & 4 & -1 & 0 & -4 & 0 \\ 0 & 1 & -2 & 4 & -1 & 0 & -4 & 0 & 2 \\ 1 & -2 & 4 & -1 & 0 & -4 & 0 & 2 & 0 \\ -2 & 4 & -1 & 0 & -4 & 0 & 2 & 0 & 1 \\ 4 & -8 & -5 & -5 & 7 & 7 & 1 & 1 & -2 \\ 1 & 1 & -2 & 1 & 1 & -2 & 1 & 1 & -2 \\ 1 & -2 & 1 & 1 & -2 & 1 & 1 & -2 & 1 \\ c & c & c & c & c & c & c & c & c \end{pmatrix}, \quad c = -3/4.$$

The first 8 rows correspond to the divisors of the functions

$$\frac{E_1 E_{11}}{E_2 E_8}, \quad \frac{E_2 E_5}{E_4 E_{11}}, \quad \frac{E_4 E_{10}}{E_8 E_5}, \quad \frac{E_8 E_7}{E_{11} E_{10}}, \quad \frac{E_{11} E_{13}}{E_5 E_7}, \quad \frac{E_5^3}{E_{13}^3}, \quad \frac{E_1^{(9)}(3\tau)}{E_2^{(9)}(3\tau)}, \quad \frac{E_2^{(9)}(3\tau)}{E_4^{(9)}(3\tau)}.$$

The determinant of Q is $-4252257/4$. Thus, by Lemma 6, the index is $4252257/4 \times 4/27 = 3^3 \cdot 19 \cdot 307$, which is indeed what one would get from (7). We now determine the structure of the divisor class group $\mathscr{D}_1^\infty(27)/\operatorname{div}\mathscr{F}_1^\infty(27)$.

Let P_i denote the cusps $2^{i-1}/27$. Let Q' be the 8×9 matrix formed by deleting the last row of Q. Then the Hermite normal form for Q' is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & -1 & 13842 & -13842 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -19882 & 19881 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2511 & -2512 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & -17037 & 17037 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 11942 & -11943 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 7047 & -7048 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & -22245 & 22242 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 52497 & -52497 \end{pmatrix}.$$

From this we see that the divisor class group is isomorphic to $C_{52497} \times C_3$, and generated by the classes of

$$v_1 = (P_8) - (P_9), \qquad v_2 = (P_7) - 7415(P_8) + 7714(P_9).$$

Furthermore, for a divisor $\sum_{i=1}^9 d_i(P_i)$ of degree 0, we have

$$\sum_{i=1}^9 d_i(P_i) \sim (-6427d_1 + 19882d_2 - 2511d_3 + 24452d_4 - 11942d_5 - 7047d_6$$
$$+ 7415d_7 + d_8)v_1 + (d_1 + d_4 + d_7)v_2.$$

The divisor is principal if and only 52497 and 3 divide the coefficients of v_1 and v_2, respectively.

Theorem 3. *Let $k \geq 3$ and $N = 2^k$. Let a be a generator of the cyclic group $(\mathbb{Z}/2^k\mathbb{Z})^\times/\pm 1$. For $\ell \geq 2$, set $\phi_\ell = \phi(2^\ell)/2 = 2^{\ell-2}$. Then a basis for $\mathscr{F}_1^\infty(2^k)$ modulo $\mathbb{C}^\times$ is given by*

$$\begin{cases} f_i = \dfrac{E_{a^{i-1}}E_{a^{i+\phi_{k-1}}}}{E_{a^i}E_{a^{i+\phi_{k-1}-1}}}, & i = 1, \ldots, \phi_k - \phi_{k-1} - 1, \\[2mm] f_i = \dfrac{E_{a^{i-1}}^{2^k}}{E_{a^{i+\phi_{k-1}-1}}^2}, & i = \phi_k - \phi_{k-1}, \\[2mm] f_i = \dfrac{E_{a^{i-1}}^{(2^{k-1})}(2\tau)}{E_{a^{i+\phi_{k-2}-1}}^{(2^{k-1})}(2\tau)}, & i = \phi_k - \phi_{k-1} + 1, \ldots, \phi_k - \phi_{k-2}, \\[2mm] \vdots & \vdots \\[2mm] f_i = \dfrac{E_{a^{i-1}}^{(8)}(2^{k-3}\tau)}{E_{a^i}^{(8)}(2^{k-3}\tau)}, & i = \phi_k - 1. \end{cases}$$

Proof. Let M be the matrix whose (i,j)-entry is $2^{k-1}B_2(a^{i+j-2}/2^k)$. The proof follows exactly the same way as the odd prime power case, except for that the matrices V_ℓ and U_ℓ in (15) and (17) are defined only for $3 \leq \ell \leq k$. Then the first $\phi_k - 1$ rows of $U_3 \ldots U_{k-1}U_k M$ will be the orders of the functions f_i, $i = 1, \ldots, \phi_k - 1$, at the cusps $a^{j-1}/2^k$, while the entries in the last row are all $2^{k-4}B_{2,\chi_0}$. We then use the determinant argument to show that $\{f_i\}$ is a basis. We omit the details here. $\qquad\square$

Example. Let $N = 32$ and $a = 3$. We set

$$M = (M_{ij})_{i,j=1,\ldots,8}, \quad M_{i,j} = 32B_2\left(\frac{3^{i+j-2}}{32}\right),$$

$$U_5 = \begin{pmatrix} 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \end{pmatrix}, \quad U_5' = \begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$U_4 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 \end{pmatrix}, \quad U_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \end{pmatrix}.$$

Then we have

$$Q = U_3U_4U_5'U_5M = \begin{pmatrix} 1 & 3 & -2 & 5 & -1 & -3 & 2 & -5 \\ 3 & -2 & 5 & -1 & -3 & 2 & -5 & 1 \\ -2 & 5 & -1 & -3 & 2 & -5 & 1 & 3 \\ 3 & -7 & -5 & 1 & -3 & 7 & 5 & -1 \\ 3 & 1 & -3 & -1 & 3 & 1 & -3 & -1 \\ 1 & -3 & -1 & 3 & 1 & -3 & -1 & 3 \\ 2 & -2 & 2 & -2 & 2 & -2 & 2 & -2 \\ c & c & c & c & c & c & c & c \end{pmatrix}, \quad c = -1/3,$$

where the first 7 rows correspond to the order of the functions

$$\frac{E_1 E_{13}}{E_3 E_{15}}, \quad \frac{E_3 E_7}{E_9 E_{13}}, \quad \frac{E_9 E_{11}}{E_5 E_7}, \quad \frac{E_5^2}{E_{11}^2}, \quad \frac{E_1^{(16)}(2\tau)}{E_7^{(16)}(2\tau)}, \quad \frac{E_3^{(16)}(2\tau)}{E_5^{(16)}(2\tau)}, \quad \frac{E_1^{(8)}(4\tau)}{E_3^{(8)}(4\tau)}$$

at cusps $3^{j-1}/32$, $j = 1, \ldots, 8$. From this we deduce that the class number is $2^6 \cdot 3^2 \cdot 5 \cdot 97 = 279360$, as expected.

Let P_j, $j = 1, \ldots, 8$, denote the cusps $3^{j-1}/32$. We now determine the structure of the divisor class group. Essentially, this amounts to computing the Hermite normal form for Q. Let Q' be the 7×8 matrix formed by deleting the last row of Q. Then there is a unimodular matrix U such that

$$UQ' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 2 & -4754 & 4750 \\ 0 & 1 & 0 & 0 & 0 & 3 & -5336 & 5332 \\ 0 & 0 & 1 & 0 & 0 & -4 & -3865 & 3868 \\ 0 & 0 & 0 & 1 & 0 & -4 & 2536 & -2533 \\ 0 & 0 & 0 & 0 & 2 & 2 & -354 & 350 \\ 0 & 0 & 0 & 0 & 0 & 12 & 552 & -564 \\ 0 & 0 & 0 & 0 & 0 & 0 & 11640 & -11640 \end{pmatrix}.$$

From this we see that the divisor class group $\mathscr{D}_1^\infty(32)/\operatorname{div}\mathscr{F}_1^\infty(32)$ is isomorphic to $C_{11640} \times C_{12} \times C_2$, where each component is generated by

$$v_1 = (P_7) - (P_8), \quad v_2 = (P_6) + 46(P_7) - 47(P_8), \quad v_3 = (P_5) + (P_6) - 177(P_7) + 175(P_8),$$

respectively. Moreover, for a divisor $\sum_{i=1}^8 d_i(P_i)$ of degree 0, we have

$$\sum_{i=1}^8 d_i(P_i) \sim (4623d_1 + 5474d_2 + 3681d_3 - 2720d_4 + 223d_5 - 46d_6 + d_7)v_1$$

$$+ (-d_1 - 3d_2 + 4d_3 + 4d_4 - d_5 + d_6)v_2 + (-d_1 + d_5)v_3,$$

and it is principal if and only if the three coefficients are congruent to 0 modulo 11640, 12, and 2, respectively.

4. NON-PRIME POWER CASES

4.1. Squarefree cases. Here we consider squarefree composite cases.

Theorem 4. *Let N be a composite squarefree integer, and set*

(19)
$$S = \{g_1, \ldots, g_{\phi(N)/2}\} = \{g : \ 1 \le g \le N/2, \ (g, N) = 1\}.$$

For each integer g in S and each proper divisor k of N, define $g(k)$ to be the unique integer satisfying

$$\begin{cases} g(k) \equiv 0 & \mod k, \\ g(k) \equiv \pm g & \mod N/k, \end{cases}$$

in the range $1 \le g(k) \le N/2$. For $g \in S$, set

(20)
$$F_g^{(N)}(\tau) = F_g(\tau) = \prod_{k|N, k\neq N} E_{g(k)}^{(N)}(\tau)^{\mu(k)},$$

where $\mu(k)$ is the Mobius function. Then a basis for $\mathscr{F}_1^\infty(N)$ modulo scalars is $F_{g_i}^{(N)}/F_{g_{i+1}}^{(N)}$, $i = 1, \ldots, \phi(N)/2 - 1$.

Proof. We first show that any quotient F_{g_i}/F_{g_j} of two functions F_g satisfies the orbit condition (11), which by Theorem B implies that F_{g_i}/F_{g_j} is in $\mathscr{F}_1^\infty(N)$.

Let p be a prime divisor of N and g be an integer relatively prime to N. Since N is squarefree, we may write F_g as

$$F_g = \prod_{p\nmid k} E_{g(k)}^{\mu(k)} \prod_{p|k, k\neq N} E_{g(k)}^{\mu(k)} = E_{g(N/p)}^{\mu(N/p)} \prod_{p\nmid k, k\neq N/p} E_{g(k)}^{\mu(k)} E_{g(pk)}^{-\mu(k)}.$$

For divisors k of N that are not divisible by p, the integers $g(k)$ and $g(pk)$ satisfy

$$\begin{cases} g(k) \equiv 0 & \mod k, \\ g(k) \equiv \pm g & \mod N/k, \end{cases} \qquad \begin{cases} g(pk) \equiv 0 & \mod pk, \\ g(pk) \equiv \pm g & \mod N/(pk). \end{cases}$$

Combining these congruences, we find

$$g(k) \equiv \pm g(pk) \mod N/p.$$

Therefore, F_{g_i}/F_{g_j} satisfies (11). We now show that $\mathscr{F}_1^\infty(N)$ is generated by $F_{g_i}/F_{g_{i+1}}$, $i = 1, \ldots, \phi(N)/2 - 1$. It suffices to prove that every function in $\mathscr{F}_1^\infty(N)$ is a product of F_g.

By Theorem B, every function in $\mathscr{F}_1^\infty(N)$ is of the form $f(\tau) = \prod_g E_g^{e_g}$ up to a scalar, where e_g satisfy

$$\sum_{g\in\mathcal{O}_{a,p}} e_g = 0$$

for each prime divisor p of N and each integer a. Now let p be a prime divisor of N and g be an integer in the range $1 \le g \le N/2$ satisfying $(g, N) = p$. Consider the set

$$T = \mathcal{O}_{g,p} = \{1 \le h \le N/2 : \ h \equiv \pm g \mod N/p\}.$$

Except for g itself, all elements of T are relatively prime to N. It follows that for g with $(g, N) = p$,

$$(21) \qquad e_g = - \sum_{h \equiv \pm g \bmod N/p, \ (h,N)=1} e_h,$$

where h runs over all integers in the range $1 \leq h \leq N/2$ satisfying the stated conditions.

Likewise, if p_1 and p_2 are two distinct prime divisors of N, then for all g with $1 \leq g \leq N/2$ and $(g, N) = p_1 p_2$, the set

$$T = \{1 \leq h \leq N/2 : \ h \equiv \pm g \mod N/(p_1 p_2)\}$$

can be partitioned into a union of 4 disjoint subsets

$$T = T_1 \cup T_{p_1} \cup T_{p_2} \cup T_{p_1 p_2},$$

where

$$T_k = \{h \in T : \ (h, N) = k\}.$$

Then condition (11) yields

$$\sum_{h \in T_1} e_h + \sum_{h \in T_{p_1}} e_h + \sum_{h \in T_{p_2}} e_h + \sum_{h \in T_{p_1 p_2}} e_h = \sum_{h \in T} e_h = 0.$$

Now the set $T_{p_1 p_2}$ consists of g itself. Furthermore, by (21), we have for all $h \in T_{p_i}$, $i = 1, 2$,

$$e_h = - \sum_{\ell \equiv \pm h \bmod N/p_i, \ (\ell,N)=1} e_\ell.$$

It follows that

$$\sum_{h \in T_{p_i}} e_h = - \sum_{\ell \in T_1} e_\ell$$

since for each $\ell \in T_1$ there exists exactly one element $h \in T_{p_i}$ such that $h \equiv \pm \ell$ mod N/p_i. Summarizing, we find, for all g with $(g, N) = p_1 p_2$.

$$e_g = \sum_{h \in T_1} e_h = \sum_{h \equiv \pm g \bmod N/p_1 p_2, \ (h,N)=1} e_h.$$

In general, following the same argument, we can prove by induction that if $p_1, \ldots, p_k$ are distinct prime factors of N, then for all g with $1 \leq g \leq N/2$, we have

$$(22) \qquad e_g = (-1)^{\mu(\gcd(g,N))} \sum_{h \equiv \pm g \bmod N/(g,N), \ (h,N)=1} e_h,$$

where the summation runs over all integers h satisfying $1 \leq h \leq N/2$ and the stated conditions. From this we see that

$$(23)$$
$$f(\tau) = \prod_g E_g^{e_g} = \prod_{d|N, \ d \neq N} \prod_{(g,N)=d} E_g^{e_g} = \prod_{d|N, \ d \neq N} \prod_{(g,N)=d} \prod_{\substack{h \equiv \pm g \bmod N/d \\ (h,N)=1}} E_g^{\mu(d)e_h}$$

$$= \prod_{(h,N)=1} \prod_{d|N, \ d \neq N} E_{h(d)}^{\mu(d)e_h} = \prod_{(h,N)=1} F_h^{e_h}.$$

This completes the proof of the theorem. $\qquad\qquad\square$

Example. Consider $N = 42$. Following Theorem 4, we set

$$F_1 = \frac{E_1 E_6 E_{14} E_{21}}{E_{20} E_{15} E_7}, \quad F_5 = \frac{E_5 E_{12} E_{14} E_{21}}{E_{16} E_9 E_7}, \quad F_{11} = \frac{E_{11} E_{18} E_{14} E_{21}}{E_{10} E_3 E_7},$$

$$F_{13} = \frac{E_{13} E_6 E_{14} E_{21}}{E_8 E_{15} E_7}, \quad F_{17} = \frac{E_{17} E_{18} E_{14} E_{21}}{E_4 E_3 E_7}, \quad F_{19} = \frac{E_{19} E_{12} E_{14} E_{21}}{E_2 E_9 E_7}.$$

According to Theorem 4, the group $\mathscr{F}_1^\infty(42)$, up to scalars, is generated by

$$f_1 = \frac{F_1}{F_5}, \quad f_2 = \frac{F_5}{F_{11}}, \quad f_3 = \frac{F_{11}}{F_{13}}, \quad f_4 = \frac{F_{13}}{F_{17}}, \quad f_5 = \frac{F_{17}}{F_{19}}.$$

To check the correctness, we form a 6×6 matrix

$$M = \begin{pmatrix} 5 & 9 & -5 & 6 & -14 & -1 \\ 6 & -8 & -1 & 2 & 12 & -11 \\ 5 & -6 & 9 & -14 & -1 & 5 \\ 8 & -12 & -2 & 11 & -6 & 1 \\ -2 & 11 & -12 & -6 & 1 & 8 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

whose first 5 rows are the orders of f_i at $1/42$, $5/42$, $11/42$, $13/42$, $17/42$, and $19/42$, respectively. We have $\det(M)/6 = 248430$, which agrees with the class number obtained from Yu's formula.

To determine the group structure of generators of the divisor class group, we remove the last row of M and put it in the Hermite normal form. Explicitly, we have

$$\begin{pmatrix} -4 & -53 & 37 & 71 & 22 \\ 0 & 6 & -2 & -6 & -1 \\ -3 & -33 & 25 & 46 & 15 \\ 6 & 46 & -42 & -71 & -26 \\ 11 & 142 & -99 & -190 & -59 \end{pmatrix} M = \begin{pmatrix} 1 & 0 & 0 & 1 & -1021 & 1019 \\ 0 & 1 & 0 & -20 & 109 & -90 \\ 0 & 0 & 1 & -18 & -640 & 657 \\ 0 & 0 & 0 & 91 & 910 & -1001 \\ 0 & 0 & 0 & 0 & 2730 & -2730 \end{pmatrix},$$

where the 5×5 matrix on the left is a unimodular matrix. (We have removed the last row of M.) From this we see that the divisor class group is isomorphic to $C_{2730} \times C_{91}$, whose components are generated by the classes of

$$(17/42) - (19/42), \qquad (13/42) + 10(17/42) - 11(19/42),$$

respectively.

Remark. We remark that one can actually use Theorem 4 to give another proof of Theorem A for squarefree integers N. The key is the distribution relation (6) of Lemma 5. For example, let us consider the case $N = 21$.

Let $b_{g,a}$ denote the numbers $21 B_2(ag/21)/2$, which is the order of E_g at $a/21$ when $(a, 21) = 1$. By Lemma 5, we have

$$3(b_{1,a} + b_{8,a} + b_{6,a}) = b_{3,a},$$
$$3(b_{2,a} + b_{9,a} + b_{5,a}) = b_{6,a},$$
$$3(b_{4,a} + b_{10,a} + b_{3,a}) = b_{9,a},$$

and

$$7(b_{1,a} + b_{4,a} + b_{7,a} + b_{10,a} + b_{8,a} + b_{5,a} + b_{2,a}) = b_{7,a}$$

for all integers a. From these relations, we obtain

$$\begin{pmatrix} b_{6,a} \\ b_{9,a} \\ b_{3,a} \end{pmatrix} = -\frac{1}{3^3 - 1} \begin{pmatrix} 27 & 3 & 9 \\ 9 & 27 & 3 \\ 3 & 9 & 27 \end{pmatrix} \begin{pmatrix} b_{1,a} + b_{8,a} \\ b_{2,a} + b_{5,a} \\ b_{4,a} + b_{10,a} \end{pmatrix},$$

and

$$b_{7,a} = -\frac{7}{7 - 1}(b_{1,a} + b_{2,a} + b_{4,a} + b_{5,a} + b_{8,a} + b_{10,a}).$$

Set

$$F_1 = \frac{E_1}{E_6 E_7}, \quad F_2 = \frac{E_2}{E_9 E_7}, \quad F_4 = \frac{E_4}{E_3 E_7}, \quad F_5 = \frac{E_5}{E_9 E_7}, \quad F_8 = \frac{E_8}{E_6 E_7}, \quad F_{10} = \frac{E_{10}}{E_3 E_7}.$$

Now let M be the 6×6 matrix whose (i,j)-entry is the order $21B_2(2^{i+j-2}/21)/2$ of $E_{2^{i-1}}$ at the cusp $2^{j-1}/21$. Then the orders of $F_1, F_2, F_4, F_8, F_5, F_{10}$ at the cusps $2^{j-1}/21$ will be

$$(V_1 - V_3 - V_7)M,$$

where V_1 is the identity matrix of size 6,

$$V_3 = -\frac{1}{3^3 - 1} \begin{pmatrix} W_3 & W_3 \\ W_3 & W_3 \end{pmatrix}, \qquad W_3 = \begin{pmatrix} 27 & 3 & 9 \\ 9 & 27 & 3 \\ 3 & 9 & 27 \end{pmatrix},$$

and V_7 is the 6×6 matrix whose entries are all $-7/6$. Then the orders of the generators $F_1/F_2, F_2/F_4, F_4/F_8, F_8/F_5, F_5/F_{10}$ will make up the first 5 rows of

$$Q = \begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} (V_1 - V_3)(V_1 - V_7)M.$$

(Note that $V_3 V_7 M$ has the same number $7/2$ in every entry. Thus, the term $V_3 V_7 M$ does not contribute anything to the first 5 rows of Q.) By a direct computation and Lemma 7, the determinant of Q is equal to

$$\det Q = \cdot(1 + 3^3) \cdot (1 + 7) \cdot \prod_\chi \frac{1}{4} B_{2,\chi},$$

where χ runs over all even Dirichlet characters modulo 21. We then check that the sum of the entries in the last row of Q is

$$16 = \frac{1}{2}(1 + 3)(1 + 7) = \frac{1}{4} B_{2,\chi_0}(1 + 3)(1 + 7).$$

Thus, by Lemma 6, the class number $h_1^\infty(21)$ is equal to

$$\frac{1}{16} \det Q = \frac{1 + 3^3}{1 + 3} \cdot \frac{1 + 7}{1 + 7} \cdot \prod_{\chi \neq \chi_0} \frac{1}{4} B_{2,\chi},$$

which is (8) for $N = 21$.

In general, if $N = p_1 \dots p_n$ is a squarefree integer with $n \geq 2$, we may deduce Yu's formula using the same argument as above. Let $a_1, \dots, a_{\phi(N)/2}$ be the integers in the range $1 \leq a_i \leq N/2$ that are relatively prime to N. Let M be the matrix whose (i,j)-entry is $NB_2(a_i a_j/N)/2$ so that the ith row of M encodes the order of E_{a_i} at a_j/N. Now for each divisor k of N, using the distribution relation (6),

we can record the order of $E_{a_i(k)}$ at a_j/N in a matrix of the form $V_k M$. Then the order of F_{a_i} at a_j/N will be the (i,j)-entry of

$$\left(\sum_{k|N,\ k\neq N} \mu(k)V_k \right) M$$

We then show that the matrices V_k satisfy

$$V_{k_1} V_{k_2} = V_{k_2} V_{k_1}$$

for divisors k_1 and k_2 of N that are relatively prime and

$$\det(V_1 - V_{p_i}) = (1 + f_{p_i})^{e_{p_i}},$$

where f_{p_i} and e_{p_i} are defined as in Theorem A'. Then following the argument in the special case $N = 21$ above, one can deduce Theorem A' for composite squarefree integers N.

4.2. **Remaining cases.** In this section we give a basis $\mathscr{G}$ for $\mathscr{F}_1^\infty(N)$ for non-squarefree integers N that are not prime powers.

Let $L = \prod_{p|N} p$ be the product of distinct prime divisors of N. For each divisor M of N that is a multiple of L, we will construct a set $\mathscr{G}^{(M)}$ of modular functions in $\mathscr{F}_1^\infty(M)$ so that the union

$$\bigcup_{M:\ M|N,\ L|M} \{f(N\tau/M):\ f(\tau) \in \mathscr{G}^{(M)}\}$$

forms a basis for $\mathscr{F}_1^\infty(N)$ modulo scalars. The definition of $\mathscr{G}^{(M)}$ is given as follows.

When $M = L$ is squarefree, we define the set $\mathscr{G}^{(L)}$ to be the basis for $\mathscr{F}_1^\infty(L)$ given in Theorem 4. When $M \neq L$, M is non-squarefree. Let $p_1, \ldots, p_\ell$ be the prime divisors of M such that $p_i^2 | M$, $i = 1, \ldots, \ell$, and let $p_{\ell+1}, \ldots, p_k$ be the other prime factors of M. Set

$$K = \prod_{i=\ell+1}^{k} p_i.$$

($K = 1$ if M is squarefull.) For an integer g relatively prime to M and a divisor k of K, we let $g(k)$ be the unique integer satisfying

$$\begin{cases} g(k) \equiv 0, & \mod k, \\ g(k) \equiv \pm g, & \mod M/k, \end{cases}$$

in the range $1 \leq g(k) \leq M/2$, and set

(24) $$F_g^{(M)}(\tau) = \prod_{k|K} E_{g(k)}^{(M)}(\tau)^{\mu(k)}.$$

For each integer g in the range $1 \leq g < M/(2\prod_{i=1}^{\ell} p_i)$ satisfying $(g, M) = 1$ and each integer m_i with $1 \leq m_i \leq p_i - 1$, $i = 1, \ldots, \ell$, we set

(25) $$G_{g,m_1,\ldots,m_\ell}^{(M)}(\tau) = \prod_{(n_1,\ldots,n_\ell)\in\{0,1\}^\ell} F_{g+n_1 m_1 M/p_1 + \cdots + n_\ell m_\ell M/p_\ell}^{(M)}(\tau)^{(-1)^{n_1+\cdots+n_\ell}}.$$

Then we define the set $\mathscr{G}^{(M)}$ to be the set of all such functions

$$\mathscr{G}^{(M)} = \left\{ G_{g,m_1,\ldots,m_\ell}^{(M)}(\tau) :\ 1 \leq g \leq \frac{M}{2\prod_{i=1}^{\ell} p_i},\ (g, L) = 1,\ 1 \leq m_i \leq p_i - 1 \right\}.$$

Example. Let $M = 180 = 2^2 \cdot 3^2 \cdot 5$. We have $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, and $K = 5$. Then $\mathscr{G}^{(M)}$ consists of 8 functions $G_{1,1,m}^{(M)}$, $G_{7,1,m}^{(M)}$, $G_{11,1,m}^{(M)}$, and $G_{13,1,m}^{(M)}$ with $m = 1, 2$. Among them, the function $G_{1,1,2}^{(M)}$ is defined as

$$G_{1,1,2}^{(M)} = \frac{F_1^{(M)} F_{1+M/2+2M/3}^{(M)}}{F_{1+M/2}^{(M)} F_{1+2M/3}^{(M)}} = \frac{F_1^{(M)} F_{31}^{(M)}}{F_{91}^{(M)} F_{121}^{(M)}},$$

where $F_1^{(M)} = E_1/E_{35}$, $F_{31}^{(M)} = E_{31}/E_5$, $F_{91}^{(M)} = E_{91}/E_{55}$, and $F_{121}^{(M)} = E_{59}/E_{85}$. Thus, we have

$$G_{1,1,2}^{(M)} = \frac{E_1 E_{31} E_{55} E_{85}}{E_{91} E_{59} E_{35} E_5}.$$

The definition of $\mathscr{G}^{(M)}$ stems from the following observations.

Lemma 12. *Let the notations K, L, M, $p_1, \ldots, p_\ell$, and $p_{\ell+1}, \ldots, p_k$ be given as above. For any g relatively prime to M and any j with $1 \le j \le \ell$, the elements in the orbit*

$$\mathcal{O}_{g,p_1 \ldots p_j} = \{h \mod M : g \equiv h \mod M/(p_1 \ldots p_j)\}/ \pm 1$$

can be uniquely represented by

$$(26) \qquad g + m_1 \frac{M}{p_1} + \cdots + m_j \frac{M}{p_j}, \quad 0 \le m_i \le p_i - 1.$$

Proof. Write $P = p_1 \ldots p_j$. We first show that $|\mathcal{O}_{g,P}| = P$, that is, all numbers $g + kM/P$ are distinct under the identification $\mathbb{Z}/M\mathbb{Z} \to (\mathbb{Z}/M\mathbb{Z})/ \pm 1$. Suppose that $g \equiv -g - kM/P \mod M$ for some k. Then we have $2g \equiv 0 \mod M/P$, which is impossible since $M/P \ge p_1 \ldots p_\ell \ge 6$ and g is assumed to be relatively prime to M.

Now it is obvious that every number in (26) is congruent to g modulo M/P, and the number of elements in (26) is the same as $|\mathcal{O}_{g,P}| = P$. Thus, we only need to show that two different elements in (26) can not be congruent to each other modulo M/P. This can be achieved by considering the reduction modulo $p_i^{n_i-1}$ for various p_i, where $p_i^{n_i}$ denotes the exact power of p dividing M. $\qquad\square$

Lemma 13. *Let all the notations be given as above. Assume that $\prod_g E_g^{e_g} \in \mathscr{F}_1^\infty(M)$. Then, for any integer g relatively prime to M and any integer j with $1 \le j \le \ell$, we have the relation*

$$(27) \quad e_g = \sum_{P|p_1 \ldots p_j} \mu(P) \sum_{h \in \mathcal{O}_{g,P}} e_h = (-1)^j \sum_{m_1=1}^{p_1-1} \cdots \sum_{m_j=1}^{p_j-1} e_{g+m_1 M/p_1 + \cdots + m_j M/p_j}$$

for e_g.

Proof. We start by considering the first equality in (27). For the case $j = 1$, it is an immediate consequence of the orbit condition (11). We then proceed by induction. Assume that the first equality of (27) holds up to j with $j < \ell$, that is,

$$e_g = \sum_{P|p_1 \ldots p_j} \mu(P) \sum_{h \in \mathcal{O}_{g,P}} e_h.$$

Then we have, by the induction hypothesis,

$$e_g = \sum_{P|p_1\ldots p_j} \mu(P) \sum_{h\in\mathcal{O}_{g,P}} \left(\sum_{k\in\mathcal{O}_{h,1}} e_k - \sum_{k\in\mathcal{O}_{h,p_{j+1}}} e_k \right).$$

The orbit $\mathcal{O}_{h,1}$ contains h itself. Also, by Lemma 12 above, we have

$$\sum_{h\in\mathcal{O}_{g,P}} \sum_{k\in\mathcal{O}_{h,p_{j+1}}} e_k = \sum_{h\in\mathcal{O}_{g,p_{j+1}P}} e_h.$$

It follows that

$$e_g = \sum_{P|p_1\ldots p_j} \mu(P) \left(\sum_{h\in\mathcal{O}_{g,P}} e_h - \sum_{h\in\mathcal{O}_{g,p_{j+1}P}} e_h \right) = \sum_{P|p_1\ldots p_{j+1}} \mu(P) \sum_{h\in\mathcal{O}_{g,P}} e_h.$$

This proves the first equality of (27). We now prove the second equality.

Regardless of what P is, the elements h in $\mathcal{O}_{g,P}$ always take the form

$$h = g + m_1\frac{M}{p_1} + \cdots + m_j\frac{M}{p_j}$$

for some m_i with $0 \le m_i < p_i - 1$. In the other direction, such an element h can appear in $\mathcal{O}_{g,P}$ if and only if for all i with $m_i \ne 0$, p_i divides P. Thus, let $Q = \prod_{i:m_i\ne 0} p_i$. Then the coefficient of e_h in (27) is equal to

$$\sum_{P|p_1\ldots p_j, Q|P} \mu(P),$$

which is $(-1)^j$ if $Q = p_1\ldots p_j$ and 0 if $Q \ne p_1\ldots p_j$. This gives the second equality of (27). $\qquad\square$

We now verify that $G^{(M)}_{g,m_1,\ldots,m_\ell}(\tau)$ are modular functions contained in $\mathscr{F}_1^\infty(M)$.

Lemma 14. *Let the notations be given as above. Then the functions $G^{(M)}_{g,m_1,\ldots,m_\ell}$ are modular functions contained in $\mathscr{F}_1^\infty(M)$.*

Proof. The case when $M = L$ is squarefree is verified in Theorem 4. For other M, using the argument given in the first paragraph of the proof of Theorem 4, we see that for all prime factors q of M satisfying $q^2 \nmid M$, the functions F_g all satisfy condition (11). For prime factors p of M satisfying $p^2|M$, it is clear from our definition that $G^{(M)}_{g,m_1,\ldots,m_\ell}$ satisfy condition (11). Therefore, by Theorem B, the functions $G^{(M)}_{g,m_1,\ldots,m_\ell}$ are all modular functions contained in $\mathscr{F}_1^\infty(M)$. $\qquad\square$

Corollary 15. *Let all the notations be given as above. Define*

(28) $$\mathscr{G}^{(M)}(d) = \{f(d\tau) : f(\tau) \in \mathscr{G}^{(M)}\}.$$

Then all the functions in $\mathscr{G}^{(M)}(N/M)$ are modular functions belonging to $\mathscr{F}_1^\infty(N)$.

Proof. This immediately follows from Lemmas 10 and 14. $\qquad\square$

Now we present our basis for $\mathscr{F}_1^\infty(N)$.

Theorem 5. *Let all the notations be given as above. Then a basis for $\mathscr{F}_1^\infty(N)$ modulo $\mathbb{C}^\times$ is*

$$\bigcup_{M:\ M|N,\ L|M} \mathscr{G}^{(M)}(N/M),$$

where $\mathscr{G}^{(M)}(N/M) = \{f(N\tau/M) :\ f(\tau) \in \mathscr{G}^{(M)}\}$.

Example. Consider the case $N = p^a q^b$, where p and q are distinct primes and $a, b \geq 1$. Let us compute the number of elements in $\mathscr{G}^{(p^i q^j)}$ for $i, j \geq 1$.

When $2 \leq i \leq a$ and $2 \leq j \leq b$, the set

$$\mathscr{G}^{(p^i q^j)} = \{G_{g,m_1,m_2}^{(p^i q^j)} : 1 \leq g \leq p^{i-1} q^{j-1}/2,\ (g, pq) = 1,$$
$$1 \leq m_1 \leq p-1,\ 1 \leq m_2 \leq q-1\}$$

has

$$\frac{1}{2}\phi(p^{i-1}q^{j-1}) \cdot (p-1) \cdot (q-1) = \frac{1}{2}p^{i-2}q^{j-2}(p-1)^2(q-1)^2$$

elements. When $i = 1$ and $2 \leq j \leq b$, the set

$$\mathscr{G}^{(pq^j)} = \{G_{g,m}^{(pq^j)} :\ 1 \leq g \leq pq^{j-1}/2,\ (g, pq) = 1,\ 1 \leq m \leq q-1\}$$

has $q^{j-2}(p-1)(q-1)^2/2$ elements. Likewise, when $2 \leq i \leq a$ and $j = 1$, the set $\mathscr{G}_{p^i q}$ has $p^{i-2}(p-1)^2(q-1)$ elements. When $i = 1$ and $j = 1$, the set $\mathscr{G}^{(pq)}$ has $(p-1)(q-1)/2 - 1$ elements. Thus, the set

$$\bigcup_{M:\ M|p^a q^b,\ pq|M} \mathscr{G}^{(M)}(p^a q^b/M)$$

has totally

$$\frac{1}{2}\sum_{i=2}^{a}\sum_{j=2}^{b} p^{i-2}q^{j-2}(p-1)^2(q-1)^2 + \frac{1}{2}\sum_{j=2}^{b} q^{j-2}(p-1)(q-1)^2$$

$$+ \frac{1}{2}\sum_{i=2}^{a} p^{j-2}(p-1)^2(q-1) + \frac{(p-1)(q-1)}{2} - 1$$

$$= \frac{1}{2}(p^{a-1}-1)(q^{b-1}-1)(p-1)(q-1) + \frac{1}{2}(q^{b-1}-1)(p-1)(q-1)$$

$$+ \frac{1}{2}(p^{a-1}-1)(p-1)(q-1) + \frac{1}{2}(p-1)(q-1) - 1$$

$$= \frac{1}{2}p^{a-1}q^{b-1}(p-1)(q-1) - 1,$$

which is the precisely the number of functions needed to generate $\mathscr{F}_1^\infty(p^a q^b)$.

Proof of Theorem 5. By Corollary 15, the functions in $\mathscr{G}^{(M)}(N/M)$ are all contained in $\mathscr{F}_1^\infty(N)$. To show that they generate $\mathscr{F}_1^\infty(N)$, we recall Theorem B that $f(\tau) \in \mathscr{F}_1^\infty(N)$ if and only if

$$f(\tau) = \prod_g E_g(\tau)^{e_g}$$

is a product of $E_g(\tau)$ with the exponents e_g satisfying the orbit condition (11). We will prove that such a function can be expressed as a product of functions from $\cup_M \mathscr{G}^{(M)}(N/M)$.

Let $L = \prod_{p|N} p$ be the product of distinct prime divisors of N. We start out by observing that, for each divisor d of N/L, the set

$$S_d = \{g \bmod N : \gcd(g, N/L) = d\}/\pm 1$$

is stable under the map $g \bmod N \mapsto g + N/p \bmod N$ for all prime divisor p of N since N/p is always a multiple of N/L. Thus, by Theorem B, if $f(\tau) = \prod E_g^{e_g}$ is a modular function in $\mathscr{F}_1^\infty(N)$, then so is

$$\prod_{g \in S_d} E_g^{e_g}$$

for each divisor d of N/L. Therefore, to prove the theorem, it suffices to consider the special case where $f(\tau) \in \mathscr{F}_1^\infty(N)$ takes the form $\prod_{g \in S_d} E_g^{e_g}$. We claim that such a function can be expressed as a product of functions from $\mathscr{G}^{(N/d)}(d)$.

Assume that $\prod_{g \in S_d} E_g^{e_g} \in \mathscr{F}_1^\infty(N)$. Then e_g satisfy condition (11)

$$\sum_{g \in \mathcal{O}_{a,p}} e_g = 0$$

for all a with $\gcd(a, N/L) = d$ and all prime factors p of N. This condition can also be written as

$$\sum_{g/d \equiv \pm b \bmod (N/d)/p} e_g = 0,$$

for all b satisfying $\gcd(b, N/(dL)) = 1$. Therefore, from Theorem B we deduce that $\prod_{g \in S_d} E_g^{(N)}(\tau)^{e_g} \in \mathscr{F}_1^\infty(N)$ if and only if $\prod_{g \in S_d} E_{g/d}^{(N/d)}(\tau)^{e_g} \in \mathscr{F}_1^\infty(N/d)$. Thus, the assertion that every function of the form $\prod_{g \in S_d} E_g^{(N)}(\tau)^{e_g}$ in $\mathscr{F}_1^\infty(N)$ is generated by $\mathscr{G}^{(N/d)}(d)$ is equivalent to the assertion that every function of the form

$$\prod_{h:\ (h, N/(dL))=1} E_h^{(N/d)}(\tau)^{e_h}$$

in $\mathscr{F}_1^\infty(N/d)$ is generated by functions from $\mathscr{G}^{(N/d)}(1) = \mathscr{G}^{(N/d)}$.

Rehashing our problem, what we need to show now is the following. Let M be a non-squarefree, non-prime power integer. Let $L = \prod_{p|M} p$ be the product of distinct prime divisors of M. Let $p_1, \ldots, p_\ell$ be the prime divisors of M such that $p_i^2 | M$ and $p_{\ell+1}, \ldots, p_k$ be the remaining prime factors of M. Set

$$K = \prod_{i=\ell+1}^{k} p_i.$$

We are required to show that if a function $f(\tau)$ in $\mathscr{F}_1^\infty(M)$ takes the form

$$f(\tau) = \prod_{g:\ (g, M/L)=1} E_g^{(M)}(\tau)^{e_g},$$

then it is a product of functions from

$$\mathscr{G}^{(M)} = \left\{ G_{g,m_1,\ldots,m_\ell}^{(M)}(\tau) : 1 \le g \le \frac{M}{2 \prod_{i=1}^{\ell} p_i}, (g, L) = 1, 1 \le m_i \le p_i - 1 \right\},$$

where $G_{g,m_1,\ldots,m_\ell}^{(M)}(\tau)$ are defined by (24) and (25).

First of all, following the deduction of (22) in the proof of Theorem 4, we find that the exponents e_g satisfy

$$e_g = (-1)^{\mu(\gcd(g,K))} \sum_{\substack{h \equiv \pm g \bmod M/(g,K), \ (h,M)=1}} e_h,$$

where h runs over all integers in the range $1 \leq h \leq M/2$ satisfying the stated congruence condition. Then the argument in (23) gives

$$(29) \qquad f(\tau) = \prod_{(g,M)=1} F_g^{(M)}(\tau)^{e_g},$$

where $F_g^{(M)}$ is defined by (24).

For convenience, we drop the superscript (M) and write $F_g^{(M)}(\tau)$ as F_g. Partitioning the product in (29) according to the orbits $\mathcal{O}_{g,p_1\dots p_\ell}$, we have

$$f(\tau) = \prod_{\substack{1 \leq g \leq M/(2p_1\dots p_\ell) \\ (g,M)=1}} \prod_{h \in \mathcal{O}_{g,p_1\dots p_\ell}} F_h^{e_h}.$$

By Lemma 12, every element h in $\mathcal{O}_{g,p_1\dots p_\ell}$ can be uniquely represented as

$$(30) \qquad h = g + m_1 \frac{M}{p_1} + \dots + m_\ell \frac{M}{p_\ell}.$$

For such an element, we define

$$Q(h) = \prod_{i: \ m_i = 0} p_i.$$

By Lemma 13, we have

$$e_h = \sum_{P|Q(h)} \mu(P) \sum_{k \in \mathcal{O}_{h,P}} e_k.$$

Notice that the second equality in (27) shows that the coefficient of e_k on the right-hand side of the above expression is nonzero if and only if the numbers n_i in

$$(31) \qquad k = g + n_1 \frac{M}{p_1} + \dots + n_\ell \frac{M}{p_\ell}$$

are all nonzero. Thus, we may write $f(\tau)$ as

$$f(\tau) = \prod_g \prod_k \left(\prod_{P|p_1\dots p_\ell} \left(\prod_{h:P|Q(h), h \in \mathcal{O}_{k,P}} F_h \right)^{\mu(P)} \right)^{e_k},$$

where g runs over all integers satisfying $1 \leq g \leq M/(2p_1\dots p_\ell)$ and $(g,M) = 1$ and k runs over all numbers of the form (31) with $n_i \neq 0$ for all i. Now consider the product over h. An integer h of the form (30) satisfies $P|Q(h)$ if and only if $p_i|P$ implies $m_i = 0$. Also, $h \in \mathcal{O}_{k,P}$ if and only if $m_j = n_j$ for all j with $p_j \nmid P$. Therefore, the only h that satisfies both $P|Q(h)$ and $h \in \mathcal{O}_{k,P}$ is

$$h = g + \sum_{1 \leq i \leq \ell, p_i \nmid P} n_i \frac{M}{p_i}.$$

Then we have

$$
\prod_{P|p_1\dots p_\ell} \left(\prod_{h:P|Q(h),h\in\mathcal{O}_{k,P}} F_h \right)^{\mu(P)}
$$
$$
= \prod_{(r_1,\dots,r_\ell)\in\{0,1\}^\ell} F^{(M)}_{g+r_1 n_1 M/p_1+\dots+r_\ell n_\ell M/p_\ell}(\tau)^{(-1)^{n_1+\dots+n_\ell}} = G^{(M)}_{g,n_1,\dots,n_\ell}(\tau),
$$

and

$$
f(\tau) = \prod_g \prod_{1\le n_i\le p_i-1} G^{(M)}_{g,n_1,\dots,n_\ell}(\tau)^{e_{g+n_1 M/p_1+\dots+n_\ell M/p_\ell}}.
$$

This completes the proof of the theorem. $\hfill\square$

Example. Let $N = 36$. In the notations of Theorem 5, we have $\mathscr{G}^{(6)} = \emptyset$ since $\phi(6)/2 - 1 = 0$. Also, when $M = 12$, we have $\ell = 1$, $p_1 = 2$, and

$$
\mathscr{G}^{(12)}(3) = \{G^{(12)}_{g,m}(3\tau) : \ 1 \le g \le 12/4, \ (g,12)=1, \ 1\le m \le 1\} = \{G^{(12)}_{1,1}(3\tau)\},
$$

where

$$
(32) \qquad G^{(12)}_{1,1}(3\tau) = \frac{F^{(12)}_1(3\tau)}{F^{(12)}_7(3\tau)} = \frac{E^{(12)}_1(3\tau)/E^{(12)}_3(3\tau)}{E^{(12)}_5(3\tau)/E^{(12)}_3(3\tau)} = \frac{E^{(12)}_1(3\tau)}{E^{(12)}_5(3\tau)}.
$$

When $M = 18$, we have $\ell = 1$, $p_1 = 3$, and

$$
\mathscr{G}^{(18)}(2) = \{G^{(18)}_{g,m}(2\tau) : \ 1 \le g \le 18/6, \ (g,18)=1, \ 1\le m \le 2\}
$$
$$
= \{G^{(18)}_{1,1}(2\tau), G^{(18)}_{1,2}(2\tau)\},
$$

where

$$
(33) \qquad G^{(18)}_{1,1}(2\tau) = \frac{F^{(18)}_1(2\tau)}{F^{(18)}_7(2\tau)} = \frac{E^{(18)}_1(2\tau)/E^{(18)}_8(2\tau)}{E^{(18)}_7(2\tau)/E^{(18)}_2(2\tau)},
$$

and

$$
(34) \qquad G^{(18)}_{1,2}(2\tau) = \frac{F^{(18)}_1(2\tau)}{F^{(18)}_{13}(2\tau)} = \frac{E^{(18)}_1(2\tau)/E^{(18)}_8(2\tau)}{E^{(18)}_5(2\tau)/E^{(18)}_4(2\tau)}.
$$

When $M = 36$, we have $\ell = 2$, $p_1 = 2$, $p_2 = 3$, and

$$
\mathscr{G}^{(36)} = \{G^{(36)}_{g,m_1,m_2}(\tau) : \ 1 \le g \le 36/12, \ (g,36)=1, \ 1\le m_1 \le 1, \ 1\le m_2 \le 2\}
$$
$$
= \{G^{(36)}_{1,1,1}(\tau), G^{(36)}_{1,1,2}(\tau)\},
$$

where

$$
(35) \qquad G^{(36)}_{1,1,1}(\tau) = \frac{F^{(36)}_1(\tau)F^{(36)}_{31}(\tau)}{F^{(36)}_{19}(\tau)F^{(36)}_{13}(\tau)} = \frac{E^{(36)}_1(\tau)E^{(36)}_5(\tau)}{E^{(36)}_{17}(\tau)E^{(36)}_{13}(\tau)},
$$

and

$$
(36) \qquad G^{(36)}_{1,1,2}(\tau) = \frac{F^{(36)}_1(\tau)F^{(36)}_{43}(\tau)}{F^{(36)}_{19}(\tau)F^{(36)}_{25}(\tau)} = \frac{E^{(36)}_1(\tau)E^{(36)}_7(\tau)}{E^{(36)}_{17}(\tau)E^{(36)}_{11}(\tau)}.
$$

By Theorem 5, the functions (32)–(36) form a basis for $\mathscr{F}_1^\infty(36)$. To check the correctness, we form a 5×6 matrix

$$M = \begin{pmatrix} 3 & -3 & -3 & 3 & 3 & -3 \\ 6 & -4 & -2 & -2 & -4 & 6 \\ 4 & 2 & -6 & -6 & 2 & 4 \\ 6 & 1 & 5 & -5 & -1 & -6 \\ 5 & 6 & -1 & 1 & -6 & -5 \end{pmatrix}.$$

whose rows consist of the orders of the above functions at $1/36$, $5/36$, $7/36$, $11/36$, $13/36$, and $17/36$. From the matrix we deduce that the class number $h_1^\infty(36)$ is equal to 31248, which agrees with what one gets using Theorem A. To determine the group structure and the generators of the divisor class group, we compute the Hermite normal form of M. We find it is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & -1540 & 1539 \\ 0 & 1 & 0 & 0 & -981 & 980 \\ 0 & 0 & 1 & -1 & 2044 & -2044 \\ 0 & 0 & 0 & 4 & -1588 & 1584 \\ 0 & 0 & 0 & 0 & 7812 & -7812 \end{pmatrix}.$$

Therefore the divisor class group is isomorphic to $C_4 \times C_{7812}$, where the components are generated by the classes of

$$(11/36) - 397(13/36) + 396(17/36), \qquad (13/36) - (17/36),$$

respectively.

Example. Consider the case $N = 40$ with $L = 10$. We have

$$\mathscr{G}^{(10)}(4) = \left\{ \frac{E_1^{(10)}(4\tau)E_2^{(10)}(4\tau)}{E_3^{(10)}(4\tau)E_4^{(10)}(4\tau)} \right\}, \qquad \mathscr{G}^{(20)}(2) = \left\{ \frac{E_1^{(20)}(2\tau)}{E_9^{(20)}(2\tau)}, \frac{E_3^{(20)}(2\tau)}{E_7^{(20)}(2\tau)} \right\},$$

and

$$\mathscr{G}^{(40)}(1) = \left\{ \frac{E_1(\tau)E_5(\tau)}{E_{15}(\tau)E_{19}(\tau)}, \frac{E_3(\tau)E_{15}(\tau)}{E_{17}(\tau)E_5(\tau)}, \frac{E_7(\tau)E_5(\tau)}{E_{13}(\tau)E_{15}(\tau)}, \frac{E_9(\tau)E_5(\tau)}{E_{11}(\tau)E_{15}(\tau)} \right\}.$$

We find that the class number $h_1^\infty(40)$ is 4775680, and the divisor class group is isomorphic to $C_{298480} \times C_4^2$.

Example. Consider $N = 72$. We have $\mathscr{G}^{(6)} = \emptyset$, $\mathscr{G}^{(12)}(6) = \{E_1^{(12)}(6\tau)/E_5^{(12)}(6\tau)\}$,

$$\mathscr{G}^{(18)}(4) = \left\{ \frac{E_1^{(18)}(4\tau)E_2^{(18)}(4\tau)}{E_7^{(18)}(4\tau)E_8^{(18)}(4\tau)}, \frac{E_1^{(18)}(4\tau)E_4^{(18)}(4\tau)}{E_5^{(18)}(4\tau)E_8^{(18)}(4\tau)} \right\},$$

$$\mathscr{G}^{(24)}(3) = \left\{ \frac{E_1^{(24)}(3\tau)E_3^{(24)}(3\tau)}{E_{11}^{(24)}(3\tau)E_9^{(24)}(3\tau)}, \frac{E_5^{(24)}(3\tau)E_9^{(24)}(3\tau)}{E_7^{(24)}(3\tau)E_3^{(24)}(3\tau)} \right\},$$

$$\mathscr{G}^{(36)}(2) = \left\{ \frac{E_1^{(36)}(2\tau)E_5^{(36)}(2\tau)}{E_{13}^{(36)}(2\tau)E_{17}^{(36)}(2\tau)}, \frac{E_1^{(36)}(2\tau)E_7^{(36)}(2\tau)}{E_{11}^{(36)}(2\tau)E_{17}^{(36)}(2\tau)} \right\},$$

and

$$\mathscr{G}^{(72)} = \left\{ \frac{E_1(\tau)E_{11}(\tau)}{E_{25}(\tau)E_{35}(\tau)}, \frac{E_1(\tau)E_{13}(\tau)}{E_{23}(\tau)E_{25}(\tau)}, \frac{E_5(\tau)E_7(\tau)}{E_{29}(\tau)E_{31}(\tau)}, \frac{E_5(\tau)E_{17}(\tau)}{E_{19}(\tau)E_{31}(\tau)} \right\}.$$

Using this basis for $\mathscr{F}_1^\infty(72)$, we find the divisor class group is isomorphic to

$$C_4 \times C_{12} \times C_{36} \times C_{144} \times C_{9146133360}.$$

5. Computational results

In this section, we give a few tables of computational results. The first table contains the group structure of $\mathscr{C}_1^\infty(N)$ for $N \leq 100$. (Note that for $N = 1, \dots, 10$ and $N = 12$, the Jacobian is trivial.) For the reader's convenience, we have also included the genus of the modular curve $X_1(N)$ and the prime factorization of the group order of $\mathscr{C}_1^\infty(N)$ for $N \leq 50$. We have used Hazama's formula (whenever applicable) and Yu's formula to check that the group orders are correct. Here the notation $[n_1, \dots, n_k]$ means that the group structure is $(\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})$.

In the second table, we give the p-parts of $\mathscr{C}_1^\infty(p^n)$ for small p^n. The notation $(p^{e_1})^{n_1} \dots (p^{e_k})^{n_k}$ means that the primary decomposition of $\mathscr{C}_1^\infty(p^n)$ contains n_i copies of $\mathbb{Z}/p^{e_i}\mathbb{Z}$. Finally, in the last table, we list the p-parts of $\mathscr{C}_1^\infty(mp^n)$ for selected integers $N = mp^n$.

TABLE 1. Group structure of $\mathscr{C}_1^\infty(N)$, $N \leq 100$

N	genus	class number	structure
11	1	5	cyclic
13	2	19	cyclic
14	1	3	cyclic
15	1	2^2	cyclic
16	2	$2 \cdot 5$	cyclic
17	5	$2^3 \cdot 73$	cyclic
18	2	7	cyclic
19	7	$3^2 \cdot 487$	cyclic
20	3	$2^2 \cdot 5$	cyclic
21	5	$2 \cdot 7 \cdot 13$	cyclic
22	6	$5 \cdot 31$	cyclic
23	12	$11 \cdot 37181$	cyclic
24	5	$2^2 \cdot 3 \cdot 5$	cyclic
25	12	$5 \cdot 71 \cdot 641$	cyclic
26	10	$3 \cdot 5 \cdot 7 \cdot 19$	cyclic
27	13	$3^3 \cdot 19 \cdot 307$	[3, 52497]
28	10	$2^6 \cdot 3 \cdot 13$	[4, 4, 156]
29	22	$2^6 \cdot 3 \cdot 7 \cdot 43 \cdot 17837$	[4, 4, 64427244]
30	9	$2^2 \cdot 5 \cdot 17$	cyclic
31	26	$2^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 2302381$	[10, 1772833370]
32	17	$2^6 \cdot 3^2 \cdot 5 \cdot 97$	[2, 12, 11640]
33	21	$2 \cdot 3 \cdot 5 \cdot 11 \cdot 61 \cdot 421$	cyclic
34	21	$2^3 \cdot 3 \cdot 5^2 \cdot 17 \cdot 73$	[5, 148920]
35	25	$2^2 \cdot 3 \cdot 5 \cdot 13^2 \cdot 31 \cdot 37 \cdot 61$	[13, 54574260]
36	17	$2^4 \cdot 3^2 \cdot 7 \cdot 31$	[4, 7812]
37	40	$3^2 \cdot 5 \cdot 7 \cdot 19 \cdot 37 \cdot 73 \cdot 577 \cdot 17209$	cyclic
38	28	$3^4 \cdot 7 \cdot 73 \cdot 487$	[9, 2239713]
39	33	$2^5 \cdot 3^4 \cdot 7^2 \cdot 13^3 \cdot 19$	[1638, 3236688]
40	25	$2^8 \cdot 5 \cdot 7 \cdot 13 \cdot 41$	[4, 4, 298480]
41	51	$2^4 \cdot 5 \cdot 13 \cdot 31^2 \cdot 431 \cdot 250183721$	cyclic
42	25	$2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 13^2$	[91, 2730]
43	57	$2^2 \cdot 7 \cdot 19 \cdot 29 \cdot 463 \cdot 1051 \cdot 416532733$	[2, 15635525329848799006]
44	36	$2^8 \cdot 5 \cdot 7 \cdot 31^2 \cdot 101$	[4, 4, 124, 438340]
45	41	$2^2 \cdot 3^6 \cdot 7 \cdot 31 \cdot 73 \cdot 3637$	[9, 9, 2074093812]
46	45	$11 \cdot 89 \cdot 683 \cdot 37181$	cyclic
47	70	$23 \cdot 139 \cdot 82397087 \cdot 12451196833$	cyclic
48	37	$2^8 \cdot 3 \cdot 5^2 \cdot 41 \cdot 73$	[4, 20, 718320]
49	69	$7^3 \cdot 113 \cdot 2437 \cdot 1940454849859$	[7, 26183855453442042671]
50	48	$5^2 \cdot 11 \cdot 31 \cdot 41 \cdot 71 \cdot 641$	cyclic

N	structure
51	[8, 1201887101691040]
52	[4, 4, 4, 4, 5823652380]
53	[18242730287918375982989127]
54	[9, 509693373]
55	[110, 8972396739917886000]
56	[4, 4, 16, 16, 528, 4427280]
57	[7, 3446644128227394822]
58	[4, 172, 4622976893220]
59	[170904152330259748129458969976817]
60	[4, 4, 80, 2174640]
61	[77, 112451320020409938235416633958157]
62	[11, 10230, 1813608537510]
63	[9, 9, 18, 23940, 36513252544860]
64	[2, 4, 4, 4, 8, 48, 73910454036960]
65	[2, 4, 4, 4, 4, 64, 69171648, 3833806702270272]
66	[341, 8669648790]
67	[661, 22816652454440471548245465354869311 7]
68	[2, 4, 4, 4, 4, 4, 340, 29034225327840]
69	[4196214854891108838250784527]
70	[13, 39, 7825676012700]
71	[701, 846772703911192558471548563811885556615]
72	[4, 12, 36, 144, 9146133360]
73	[2, 2, 99403183189313887693967220698760400373298427]
74	[87381, 1137260725252531425]
75	[25, 25, 229987489818652358805100]
76	[4, 4, 4, 4, 4, 4, 36, 939850887824333604]
77	[4, 8, 152, 456, 89190700421406700205983720927320]
78	[273, 1638, 66303553680]
79	[521, 294271001642094574850894479335331814815503017597]
80	[4, 4, 4, 4, 16, 80, 13855590960585920]
81	[3, 9, 9, 9, 9, 9, 27, 87945822520529641810558635771]
82	[155, 8525, 729055927995792711600]
83	[9868634937202917020161657253350129868704910054433319 3]
84	[4, 4, 4, 364, 3640, 2254324800]
85	[8, 16, 16, 60898642354650973477583334481850214172807]

N	structure
86	$[127, 32766, 2561568114789128749998]$
87	$[4, 8, 8, 9508866416575254198955917170280 46920]$
88	$[4, 4, 4, 4, 4, 16, 496, 5456, 271296378433899280]$
89	$[2, 2, 1675249887322939512499154702617308393108292544 1759332846930]$
90	$[3, 9, 63, 552341552604660]$
91	$[4, 8, 24, 191520, 6795471369773292492100456151143 28726306400]$
92	$[4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 1719661629517409605797 2420]$
93	$[2, 58520, 27655854146903254636965396728546654040]$
94	$[16369155754755236205559575360 05041]$
95	$[234, 234, 2872147481956126135917110117447829607394 5013520]$
96	$[4, 4, 4, 4, 48, 240, 297091975708501440]$
97	$[35, 18444835030732778123382892108430085232877549944 6274957379700139920]$
98	$[49, 783386490641061468174212253579]$
99	$[3, 9, 9, 9, 9, 9, 9, 9, 9, 117459, 18669220790360145041 2662961290630]$
100	$[4, 4, 4, 4, 4, 20, 100, 100, 110499590655821103 05500]$

TABLE 2. p-primary part of $\mathscr{C}_1^\infty(p^n)$

p^n	p-primary subgroups
2^4	(2)
2^5	$(2)(2^2)(2^3)$
2^6	$(2)(2^2)^3(2^3)(2^4)(2^5)$
2^7	$(2)(2^2)^7(2^3)(2^4)^3(2^5)(2^6)(2^7)$
2^8	$(2)(2^2)^{15}(2^3)(2^4)^7(2^5)(2^6)^3(2^7)(2^8)(2^9)$
2^9	$(2)(2^2)^{31}(2^3)(2^4)^{15}(2^5)(2^6)^7(2^7)(2^8)^3(2^9)(2^{10})(2^{11})$
3^3	$(3)(3^2)$
3^4	$(3)(3^2)^5(3^3)(3^4)$
3^5	$(3)(3^2)^{17}(3^3)(3^4)^5(3^5)(3^6)$
3^6	$(3)(3^2)^{53}(3^3)(3^4)^{17}(3^5)(3^6)^5(3^7)(3^8)$
5^2	(5)
5^3	$(5)(5^2)^7(5^3)$
5^4	$(5)(5^2)^{39}(5^3)(5^4)^7(5^5)$
7^2	$(7)(7^2)$
7^3	$(7)(7^2)^{17}(7^3)(7^4)$

TABLE 3. p-primary part of $\mathscr{C}_1^\infty(mp^n)$

mp^n	p-primary subgroups
$2 \cdot 3^2$	(1)
$2 \cdot 3^3$	$(3^2)^2$
$2 \cdot 3^4$	$(3^2)^6(3^4)^2$
$2 \cdot 3^5$	$(3^2)^{18}(3^4)^6(3^6)^2$
$2 \cdot 3^6$	$(3^2)^{54}(3^4)^{18}(3^6)^6(3^8)^2$
$2 \cdot 5^2$	(5^2)
$2 \cdot 5^3$	$(5^2)^8(5^4)$
$2 \cdot 5^4$	$(5^2)^{40}(5^4)^8(5^6)$
$2 \cdot 7$	(1)
$2 \cdot 7^2$	$(7^2)^2$
$2 \cdot 7^3$	$(7^2)^{18}(7^4)^2$
$3 \cdot 2^3$	(2^2)
$3 \cdot 2^4$	$(2^2)^2(2^4)$
$3 \cdot 2^5$	$(2^2)^4(2^4)^2(2^6)$
$3 \cdot 2^6$	$(2^2)^8(2^4)^4(2^6)^2(2^8)$
$3 \cdot 2^7$	$(2^2)^{16}(2^4)^8(2^6)^4(2^8)^2(2^{10})$
$3 \cdot 2^8$	$(2^2)^{32}(2^4)^{16}(2^6)^8(2^8)^4(2^{10})^2(2^{12})$
$3 \cdot 2^9$	$(2^2)^{64}(2^4)^{32}(2^6)^{16}(2^8)^8(2^{10})^4(2^{12})^2(2^{14})$
$4 \cdot 3^2$	(3^2)
$4 \cdot 3^3$	$(3^2)^4(3^4)$
$4 \cdot 3^4$	$(3^2)^{12}(3^4)^4(3^6)$
$4 \cdot 3^5$	$(3^2)^{36}(3^4)^{12}(3^6)^6(3^8)$
$6 \cdot 5$	(5)
$6 \cdot 5^2$	$(5)(5^2)^2(5^3)$
$6 \cdot 5^3$	$(5)(5^2)^{15}(5^3)(5^4)^2(5^5)$
$6 \cdot 7$	$(7)^2$
$6 \cdot 7^2$	$(7)^2(7^2)^3(7^3)^2$
$6 \cdot 7^3$	$(7)^2(7^2)^{34}(7^3)^2(7^4)^3(7^5)^2$

References

[1] Matthew H. Baker. Torsion points on modular curves. *Invent. Math.*, 140(3):487–509, 2000.
[2] J. Coates and A. Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.*, 39(3):223–251, 1977.
[3] Robert Coleman, Bruce Kaskel, and Kenneth A. Ribet. Torsion points on $X_0(N)$. In *Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996)*,

volume 66 of *Proc. Sympos. Pure Math.*, pages 27–49. Amer. Math. Soc., Providence, RI, 1999.

[4] Brian Conrad, Bas Edixhoven, and William Stein. $J_1(p)$ has connected fibers. *Doc. Math.*, 8:331–408 (electronic), 2003.

[5] János A. Csirik. The kernel of the Eisenstein ideal. *J. Number Theory*, 92(2):348–375, 2002.

[6] Martin Eichler and Don Zagier. *The theory of Jacobi forms*, volume 55 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1985.

[7] Fumio Hazama. Corrigendum: "Determinantal formula for the cuspidal class number of the modular curve $X_1(m)$". *J. Number Theory*, 72(1):151–152, 1998.

[8] Fumio Hazama. Determinantal formula for the cuspidal class number of the modular curve $X_1(m)$. *J. Number Theory*, 68(2):229–242, 1998.

[9] S. Klimek. *Ph. D. thesis*. University of California at Berkeley, 1975.

[10] Daniel S. Kubert. The square root of the Siegel group. *Proc. London Math. Soc. (3)*, 43(2):193–226, 1981.

[11] Daniel S. Kubert and Serge Lang. Units in the modular function field. I. *Math. Ann.*, 218(1):67–96, 1975.

[12] Daniel S. Kubert and Serge Lang. Units in the modular function field. II. A full set of units. *Math. Ann.*, 218(2):175–189, 1975.

[13] Daniel S. Kubert and Serge Lang. Units in the modular function field. III. Distribution relations. *Math. Ann.*, 218(3):273–285, 1975.

[14] Daniel S. Kubert and Serge Lang. Units in the modular function field. IV. The Siegel functions are generators. *Math. Ann.*, 227(3):223–242, 1977.

[15] Daniel S. Kubert and Serge Lang. The index of Stickelberger ideals of order 2 and cuspidal class numbers. *Math. Ann.*, 237(3):213–232, 1978.

[16] Daniel S. Kubert and Serge Lang. Units in the modular function field. V. Iwasawa theory in the modular tower. *Math. Ann.*, 237(2):97–104, 1978.

[17] Daniel S. Kubert and Serge Lang. *Modular units*, volume 244 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Science]*. Springer-Verlag, New York, 1981.

[18] Ju. I. Manin. Parabolic points and zeta functions of modular curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 36:19–66, 1972.

[19] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[20] Curt Meyer. *Die Berechnung der Klassenzahl Abelscher Körper über quadratischen Zahlkörpern*. Akademie-Verlag, Berlin, 1957.

[21] Morris Newman. Construction and application of a class of modular functions. *Proc. London. Math. Soc. (3)*, 7:334–350, 1957.

[22] Morris Newman. Construction and application of a class of modular functions. II. *Proc. London Math. Soc. (3)*, 9:373–387, 1959.

[23] A. P. Ogg. Diophantine equations and modular forms. *Bull. Amer. Math. Soc.*, 81:14–27, 1975.

[24] K. Ramachandra. Some applications of Kronecker's limit formulas. *Ann. of Math. (2)*, 80:104–148, 1964.

[25] Gilles Robert. *Unités elliptiques*. Société Mathématique de France, Paris, 1973. Bull. Soc. Math. France, Mém. No. 36, Bull. Soc. Math. France, Tome 101.

[26] Bruno Schoeneberg. *Elliptic modular functions: an introduction*. Springer-Verlag, New York, 1974. Translated from the German by J. R. Smart and E. A. Schwandt, Die Grundlehren der mathematischen Wissenschaften, Band 203.

[27] Toshikazu Takagi. The cuspidal class number formula for the modular curves $X_0(M)$ with M square-free. *J. Algebra*, 193(1):180–213, 1997.

[28] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[29] Heinrich Weber. *Lehrbuch der Algebra, Vol. III*. Chelsea, New York.

[30] Yifan Yang. Transformation formulas for generalized Dedekind eta functions. *Bull. London Math. Soc.*, 36(5):671–682, 2004.

[31] Jing Yu. A cuspidal class number formula for the modular curves $X_1(N)$. *Math. Ann.*, 252(3):197–216, 1980.

Department of Applied Mathematics, National Chiao Tung University, Hsinchu 300, TAIWAN
  E-mail address: `yfyang@math.nctu.edu.tw`